I flussi di dati transfrontalieri e le scelte delle imprese tra «Safe Harbor» e «Privacy Shield».

LA PROTEZIONE TRANSNAZIONALE DEI DATI PERSONALI

DAI "SAFE HARBOUR PRINCIPLES" AL "PRIVACY SHIELD"

A cura di
Giorgio Resta
Vincenzo Zeno-Zencovich

Consumatori e Mercato 5

Università degli Studi Roma Tre
Dipartimento di Giurisprudenza

Collana "Consumatori e Mercato"
5

LA PROTEZIONE TRANSNAZIONALE DEI DATI PERSONALI

DAI "SAFE HARBOUR PRINCIPLES" AL "PRIVACY SHIELD"

A cura di **Giorgio Resta** - **Vincenzo Zeno-Zencovich**

RomaTrE-Press
2016

Questo volume è stato realizzato nel quadro di una ricerca coordinata dalla Fondazione "Centro di iniziativa giuridica Piero Calamandrei" in materia di tutela dei dati personali e disciplina dell'Unione Europea, e la cui pubblicazione è stata finanziata dal Ministero per i Beni Culturali.

Presentazione della collana "Consumatori e Mercato"

La Collana "Consumatori e mercato", per le Edizioni Universitarie di Roma Tre all'interno del progetto di Ateneo Roma TrE-Press, intende essere una piattaforma editoriale multilingue, avente ad oggetto studi attinenti alla tutela dei consumatori e alla regolazione del mercato. L'intento è di stimolare un proficuo scambio scientifico attraverso una diretta partecipazione di studiosi appartenenti a diverse discipline, tradizioni e generazioni. Il dialogo multidisciplinare e multiculturale diviene infatti una componente indefettibile nell'àmbito di una materia caratterizzata da un assetto disciplinare ormai maturo tanto nelle prassi applicative del mercato quanto nel diritto vivente. L'attenzione viene in particolare rivolta al contesto del diritto europeo, matrice delle scelte legislative e regolamentari degli ordinamenti interni, e allo svolgimento dell'analisi su piani differenti (per estrazione scientifica e punti di osservazione) che diano conto della complessità ordinamentale attuale.

****

The "Consumer and market" series edited by Edizioni Universitarie di Roma Tre for the Roma TrE-Press project, aims at being a multilingual editorial project, which shall focus on consumer protection and market regulation studies. The series' core mission is the promotion of a fruitful scientific exchange amongst scholars from diverse legal systems, traditions and generations.This multidisciplinary and multicultural exchange has in fact become fundamental for a mature legal framework, from both the market practice and the law in action standpoints. A particular focus will be given on European law, where one can find the roots of the legislation and regulation in the domestic legal systems, and on the analysis of different levels, in line with the current complexity of this legal sector.

Hanno contribuito a questo volume

Marco Bassini, *dottorando nell'Università di Verona*
Cosimo Comella, *dirigente presso l'Ufficio del Garante per la protezione dei dati personali*
Virgilio D'Antonio, *professore nell'Università di Salerno*
Giusella Finocchiaro, *professore nell'Università di Bologna*
Giorgio Giannone Codiglione, *docente nell'Università di Palermo*
Alessandro Mantelero, *ricercatore nel Politecnico di Torino*
Paola Piroddi, *avvocato in Milano*
Oreste Pollicino, *professore nell'Università Bocconi di Milano*
Giorgio Resta, *professore nell'Università Roma Tre*
Giovanni Maria Riccio, *professore nell'Università di Salerno*
Salvatore Sica, *professore nell'Università di Salerno*
Vincenzo Zeno-Zencovich, *professore nell'Università Roma Tre*

Coordinamento editoriale:
Gruppo di Lavoro *Roma TrE-Press*

Elaborazione grafica della copertina: Mosquito mosquitoroma.it

Edizioni: Roma TrE-Press ©
Roma, Luglio 2016
ISBN: 978-88-97524-75-5

http://romatrepress.uniroma3.it

Indice

Vincenzo Zeno-Zencovich

Intorno alla decisione nel caso Schrems*: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*

SOMMARIO: 1. La crescente problematica della 'sovranità digitale'. – 2. Sovranità come giurisdizione. – 3. La sovranità sui segmenti materiali di una rete. – 4. Il 'territorio' di Internet. – 5. I precedenti del mare, del cielo, dello spazio. – 6. Le sedi internazionali per il governo delle reti digitali. – 7. Una visione d'insieme sulla 'sovranità digitale'.

1. La crescente problematica della 'sovranità digitale'

La decisione della Corte di Giustizia UE nel caso *Schrems* costituisce un passo ulteriore per l'affermazione di una 'sovranità digitale' dell'Unione Europea. Il termine 'sovranità' è qui utilizzato nel suo senso tradizionale: il potere di controllare, *de iure e de facto*, un certo spazio, le attività che ivi si svolgono, coloro che vi entrano, come tale spazio è organizzato, amministrare poteri di polizia, giudiziari e di sicurezza in tale spazio.

Quando la Corte di Giustizia nella sua decisione del 2014 nel caso *Google Spain*[1] ha affermato che (dilatando notevolmente il concetto di 'stabilimento' e swuscitando non poche perplessità sulla coerenza della decisione sui numerossisimi precedenti della Corte) Google deve considerarsi stabilita nell'Unione Europea ed è quindi soggetta al diritto UE, essa sta affermando la sovranità su entità economiche che operano all'interno dello spazio europeo, sia pure attraverso reti di telecomunicazione che consentono l'uso di Internet.

Quando la stessa Corte, un anno più tardi, afferma che il trasferimento

[1] *Google Spain v. Agencia Española de Protecciòn de Datos, Costeja*, C-131/12, of May 13, 2014. La decisione ha raccolto decine di commenti. Per una rassegna esaustiva della varie tematiche si veda il Volume speciale n. 4-5 /2014 di *Dir. Inf.*. I vari contributi sono raccolti ora in G. Resta – V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza* Google Spain, Roma TrE-Press, 2015 [disponibile on-line alla pagina http://ojs.romatrepress.uniroma3.it/index.php/oblio].

di dati personali di cittadini europei verso Stati Uniti non è lecito, essa sta affermando, in sostanza, che il trattamento dei dati personali è regolato dal diritto UE, non dal diritto di un altro Stato.

La circostanza che entrambi i casi riguardano dati personali[2] non deve trarre in inganno. Il trattamento dei dati personali è considerato uno dei tratti distintivi del sistema giuridico europeo, uno dei suoi valori pre-giuridici, contrapposti ad un approccio statunitense significativamente diverso allo stesso tema. Tuttavia ciò ha solo reso più facile – grazie anche a quel che appare una attenta selezione della priorità dei casi da esaminare[3] – per la Corte di Giustizia adottare decisioni dirompenti che sconfessano accordi di alto livello delle istituzioni comunitarie. Fino alla decisione nel caso *Google Spain* vi era la diffusa convinzione che il trattamento dei dati da parte del grande motore di ricerca, che è presente in praticamente ogni momento della nostra vita, doveva ritenersi effettuato sui 'mainframe' presenti negli Stati Uniti, e quindi non fosse soggetto alla direttiva UE sui dati personali. E il trasferimento di dati verso quel Paese era coperto dall'accordo internazionale «Safe Harbour» il quale, asseritamente, doveva garantire un analogo livello di protezione nel trattamento dei dati al di là dell'Atlantico.

In quest'ultimo caso il profilo della sovranità è molto più evidente, in quanto il *casus belli* è esplicitamente individuato nell'esercizio di poteri sovrani da parte degli Stati Uniti sui dati europei sulla base dell'irresistibile «Patriot Act».

La Corte di Giustizia dunque, a guardare le cose in una prospettiva realista, sta affermando che il Consiglio UE ha inammissibilmente rinunciato all'esercizio dei suoi poteri sovrani nello stipulare l'accordo «Safe Harbour» con gli Stati Uniti. La Corte – utilizzando la materia particolarmente sensibile dei diritti fondamentali – sta segnando il confine dei

[2] Cosa intendiamo per 'dati'? Sulla distinzione fra dati dinamici, dati statici e metadata v. T. Maurer et al., *Technological Sovereignty: Missing the Point?*, in M. Maybaum, A-M. Osula, L. Lindstrom (a cura di), *7th International Conference on Cyber Conflict*, 2015 NATO CCD COE Publications, (a p. 56) disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2004%20Technological%20Sovereignity%20-%20Missing%20the%20Point.pdf [ultimo accesso 10.7.2016].

[3] Pochi giorni prima della sentenza *Schrems*, la CGUE ha emesso due sentenze nei casi *Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság* (C-230/14) e *Smaranda Bara and Others c. Preşedintele Casei Naţionale de Asigurări de Sănătate and Others* (C-201/14). Nel primo caso si trattava della applicabilità dei diritto ungherese al trattamento dei dati personali da parte di un fornitore di servizi stabilito in Slovacchia (Il diritto UE sui dati personali è «nel senso che esso consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato»). Nel secondo caso ha statuito che il trasferimento, senza previo consenso, di dati fiscali personali ad un istituto di previdenza sociale non è consentito in base al diritto UE.

poteri sovrani e, molto chiaramente, statuendo la supremazia giudiziale su temi del più alto livello politico, come la politica internazionale. La sentenza *Schrems* richiede pertanto di essere analizzata nella prospettiva di due super-potenze internazionali che si fronteggiano per il controllo di una risorsa essenziale quale le reti globali di telecomunicazioni. Questo confronto era già emerso con riferimento ai casi SWIFT (dati delle operazioni bancarie)[4] e PNR (dati dei passeggeri del trasporto aereo)[5] nei quali, inconsapevolmente o coattivamente, i dati venivano trasmessi negli Stati Uniti e utilizzati dalle sue autorità. In questo caso si è passati ad un livello più ampio e generale perché comprende ogni sorta di dati, dalle fonti più diverse, consentendo una profilazione più accurata.

2. Sovranità come giurisdizione

Anche se questa non è la sede per una approfondita analisi della casistica giurisprudenziale e istituzionale, vale la pena osservare che non vi è alcuna ragione per la quale le reti di telecomunicazioni e tutte le attività che vi si svolgono direttamente o indirettamente non debbano formare oggetto di grande attenzione da parte delle super-potenze, considerando la loro importanza in tutti i campi. In questo contesto più generale si è tuttavia portati a considerare alcuni aspetti specifici non solo perché il punto di partenza è una decisione della più alta Corte dell'Unione Europea, ma anche perché essa deve essere confrontata con le decisioni di altre corti al di là dell'Atlantico[6]. Qui il concetto di sovranità si traduce nel termine elegante e tecnico di giurisdizione. Ma è del tutto evidente che stabilire che una Corte è competente a conoscere una certa controversia – e dunque ha giurisdizione – costituisce l'espressione di poteri sovrani, e solitamente questa decisione viene assunta direttamente dalle corti stesse. D'altronde

[4] Si v. l'accordo «tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi» in GUUE L8 del 13.1.2010.

[5] Si v. l'«Accordo tra gli USA e l'UE sull'uso e sul trasferimento del codice di prenotazione (Passenger Name Record — PNR) al Dipartimento per la sicurezza interna degli Stati Uniti» in GUUE L215 dell'11.8.2012.

[6] Si v. ad es *In re Microsoft*, 15 F. Supp. 3rd 466 (S.D.N.Y 2014) ove si è stabilito che i dati detenuti da Microsoft in Irlanda cadessero sotto la giurisdizione statunitense e dunque assoggettabili ad un mandato di acquisizione emesso sulla base dell'Electronic Communications Privacy Act, come modificato dal Patriot Act.

il potere di fissare norme si associa a quello di stabilire come, quando e in che misura tali norme possono o devono essere applicate. In questa prospettiva, anche se, per ipotesi, la Corte di Giustizia avesse statuito che l'accordo di «Safe Harbour» era perfettamente conforme al diritto comunitario, la decisione sarebbe stata comunque l'espressione di un potere sovrano. Bisogna poi aggiungere – e la notazione vale ancor più nel caso di reti di comunicazione elettronica – che non è sufficiente affermare la sovranità giacchè questa deve essere riconosciuta (o, almeno, subita) anche da altri Stati, senza contare le diverse situazioni di possibile interferenza fra giurisdizioni di cui venga negata la esclusività, ponendo questioni in ordine alla concorrenza fra di esse ed i criteri per evitare il rischio di conflitto fra decisioni. La sentenza Schrems è utile, da questo punto di vista, perché serve a scartare una certa idea delle attività sulle reti di telecomunicazione, e sul più noto protocollo di comunicazione, Internet, come se fosse a-territoriale e quindi non soggette a sovranità statale[7]. Questa idea – che risale alla prima epoca di Internet e al suo sviluppo spontaneo[8] – è stata ampiamente superata dalla progressiva espansione dell'intervento statale e dalla regolazione delle reti e delle attività che su di esse vengono condotte.

3. La sovranità sui segmenti materiali di una rete

Le reti di telecomunicazioni sono composte in larga parte da elementi fisici (cavi, centraline, elaboratori, trasmettitori) che devono essere posizionati da qualche parte all'interno del territorio dello stato. Anche quando la rete utilizza significativi segmenti di comunicazioni *wireless*, queste devono essere trasmesse e ricevute da antenne e radio-basi. Su queste componenti lo Stato esercita legittimamente i propri poteri o imponendo che operino sulla base di talune regole tecniche ed amministrative[9]. La

[7] L'idea è contestata da W. Heintschel Von Heinegg, *Legal Implications of Territorial Sovereignty in Cyberspace*, in C. Czosseck, R. Ottis, K. Ziolkowsky (a cura di), *4th International Conference on Cyber Conflict*, 2012 NATO CCD COE Publications, p.9 (disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/1_1_von_Heinegg_LegalImplicationsOfTerritorialSovereigntyInCyberspace.pdf [ultimo accesso 10.7.2016]).

[8] Tuttavia era già stata messa in discussione quasi vent'anni fa: v. T.S. WU, *Cyberspace Sovereignty? The Internet and the International System*, 10 *Harv. J. L.&Tech*. 647 (1997).

[9] In questo senso v. W. Heintschel Von Heinegg, *Legal Implications etc*.,cit. alla nt. 7, p.9 s. «La circostanza che le componenti dell'Internet si trovino nel territorio sovrano dello Stato ma formano, allo stesso tempo, parte dell'Internet globale, non indica che

circostanza che le trasmissioni siano intangibili non significa che lo Stato non possa, *de facto* e *de iure*, impedire la circolazione di taluni contenuti, l'accesso a siti stranieri, o l'accesso dall'esterno a siti interni, e in generale non possa legittimamente – come normalmente e regolarmente fanno anche i paesi democratici – controllare e acquisire il contenuti di comunicazioni digitali. Tutti questi interventi costituiscono segno evidente che gli stati – o nel caso dell'UE, entità sopra-nazionali alle quali gli Stati hanno conferito taluni poteri – esercitano i loro poteri sovrani sulle reti di telecomunicazioni, da aspetti minuti fino a interventi assai più complessi e profondi. Stabilire come i dati personali raccolti attraverso le reti di telecomunicazioni debbano e/o possono essere elaborati e a quali condizioni essi possano essere trasferiti in altri paesi costituisce semplicemente l'espressione dell'esercizio di poteri sovrani da parte e secondo uno stato di diritto. Il diritto, sotto forma di un provvedimento generale ovvero di una decisione giudiziale, stabilisce quel che legittimamente può essere fatto. Per le parti che non vi si conformano vi saranno sanzioni di progressiva incisività fino alla chiusura di talune attività e l'arresto delle persone fisiche che le svolgono.

Sarebbe ingenuo ritenere che questa manifestazione di poteri sovrani sia una particolarità del modello giuridico e politico europeo[10]. Negli Stati Uniti il governo delle reti globali è stato ed è attribuito in maniera significativa ad attori privati i quali operano all'interno del sistema giuridico statunitense. Il primo e ovvio esempio è quello di ICANN, l'organismo cui è attribuito il compito di fissare i criteri per l'attribuzione dei nomi di domino e altre procedure per l'attività attraverso Internet[11]. Ma anche quando grandi prestatori di servizi sulla rete (come Google, Facebook, E-bay, Wikipedia, ecc.), nelle loro condizioni generali di servizio statuiscono che il diritto applicabile è il diritto statunitense, spesso indicando un foro domestico, essi stanno in sostanza affermando che il diritto americano, e quindi i poteri sovrani degli Stati Uniti, governano la rete globale.

vi sia stata una rinuncia all'esercizio della giurisdizione territoriale» (così K. Ziolkowsi, *General Principles of International Law as Applicable in Cyberspace*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 135, at p.162) disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016].

[10] La preoccupazione per un crescente *Data Nationalism* è espressa da A.Chander, U.P.LE, 64 *Emory L.J* 677 (2015).

[11] L'ICANN si qualifica come una ONG ma è retta dal diritto statunitense e agisce per conto dello US Department of Commerce, al quale fa riferimento: see K. Ziolkowsi, *General Principles of International Law as Applicable in Cyberspace*, cit. alla nt. 9, p. 157.

Questo conflitto – in primo luogo un conflitto di sistemi e dunque un conflitto di ordinamenti giuridici – non appare risolubile attraverso le ben note e sperimentate regole del diritto internazionale privato e processuale[12]. Il problema, infatti, non è quello di stabilire quale diritto privato debba applicarsi al rapporto giuridico e chi sia il giudice competente. Quel che è in gioco in questi casi, invece, è la regolazione pubblica delle reti, che non può essere risolto attraverso le regole applicabili ai soggetti privati.

Utilizzando il caso deciso dalla Corte di Giustizia, la decisione non riguarda i dati personali del sig. Schrems (in ipotesi, Facebook avrebbe potuto impegnarsi ad accantonare i suoi dati e trattarli in Europa), ma piuttosto i dati personali di tutti i cittadini europei. Si tratta di una questione che non può essere affrontata e risolta attraverso gli strumenti e un contenzioso di diritti privato.

4. Il 'territorio' di Internet

Come s'è detto, la circostanza che i dati personali siano stati presi nel caso *Schrems* come oggetto di contesa con gli Stati Uniti non significa in alcun modo che i suoi effetti siano limitati a questo profilo[13]. Si può agevolmente immaginare l'estensione del diritto comunitario, e dunque della sovranità dell'UE, a operazioni di commercio fra l'Europa e gli Stati Uniti; all'applicazione del diritto europeo della proprietà intellettuale o della concorrenza a «big-data» conservati al di là dell'Atlantico ma comprendenti un numero significativo di dati 'europei'; o la possibilità e i limiti del trattamento di dati pubblici al di fuori dei confini dell'Unione[14]; fino al controverso tema della

[12] Le quali in ogni caso sono rese ancor più complesse dalla ubiquità dell'Internet v. D.J.B. Svantesson, *Sovereignty in International Law - How the Internet (Maybe) Changed Everything, But Not for Long,* in 8 *Masaryk U. J.L. & Tech*. 137 (2014). Il ragionamento è sviluppato dallo stesso A. in *A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft*, 2015 *Am.J.Int'l L.Unbound*, disponibile on-line alla pagina https://www.asil.org/blogs/new-jurisprudential-framework-jurisdiction-beyond-harvard-draft [ultimo accesso 10.7.2016].

[13] V. T. Maurer et al., *Technological Sovereignty*, cit. alla nt. 2.

[14] L'approccio prospettato da J. Daskal, *The Un-Territoriality of Data*, in *Yale L.J* (2016) è che i dati non sono connessi ad alcuno specifico territorio; e sono slegati dalla cittadinanza. Almeno nell'UE questa seconda affermazione non sembra condivisibile. La protezione dei dati personali è riconosciuta come diritto fondamentale dall'art.8 della Carta Europea dei Diritti Fondamentali e dunque si tratta di una situazione giuridica strettamente legata alla cittadinanza europea. Per le complesse questioni anche di ordine

tassazione delle attività in rete. Una delle ovvie conseguenze della decisione della Corte di Giustizia è la necessità di definire chiaramente i confini della sovranità dell'UE sulle reti di telecomunicazione.

In primo luogo, dove cominciano e dove finiscono?[15] La risposta non è ovvia considerando il gran numero di stati europei che hanno estensioni oltremare: si pensi alla Danimarca con la Groenlandia, i Paesi Bassi con i possedimenti nelle Antille, la Francia con i suoi DOM e TOM, e il Regno Unito con le dozzine di isole disseminate in ogni oceano del mondo. Si deve poi considerare che gran parte degli abitanti di tali luoghi assai distanti hanno una cittadinanza europea e dunque vantano gli stessi diritti dei cittadini della madre-patria e sono soggetti alle stesse leggi. E i cittadini – e la cittadinanza – sono uno degli elementi essenziali della sovranità[16].

Questo elemento richiede di essere attentamente considerato in una molteplicità di casi:

a. Quando un cittadino dell'Unione accede la rete dall'Europa e raggiunge un sito extra-UE

b. Quando un cittadino extra-comunitario accede, da fuori dell'Europa, un sito che ha sede in Europa.

c. Quando un cittadino europeo, che si trova al di fuori dell'Unione, accede un sito che si trova all'interno[17].

---

costituzionale che risultano dall'uso del 'cloud computing' nel campo dei dati detenuti da soggetti pubblici (e quindi oggetto di un potere sovrano di controllo e comando) e la interazione con il diritto UE v. F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. Inf.* 2015, 227 (p. 250 s.).

[15] V. P.W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 *Air Force L.Rev*. 1 (2009): «Gli stati devono essere in grado di stabilire una frontiera nel ciber-spazio che uno stato può sia sorvegliare che controllare. Se non si è in grado di svolgere tale funzione, il concetto di sovranità nel ciber-spazio è priva di significato» (p. 39).

[16] Si sostiene che nei casi in cui i dati sono trattati (asseritamente in maniera illegittima) al di fuori dell'Unione, la UE applicherebbe il principio della c.d. personalità passiva (v. B. Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 189 (a p. 196) disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016]. Per un approccio che collega giurisdizione a cittadinanza v C.RYNGAERT, M. Zoetekouw, *The End of Territory? The Re-Emergence of Community as a Principle of Jurisdictional Order in the Internet Era*, disponibile on-line alla pagina http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523354 [ultimo accesso 10.7.2016].

[17] Questo approccio è diverso da quello seguito da W. Heintschel Von Heinegg, *Legal Implications etc*., cit. alla nt.7 (p. 15) nel caso della giurisdizione nei confronti di taluno

È chiaro che la crescente tensione fra il bisogno di una rete aperta e autenticamente globale e l'affermazione di diritti di sovranità sul proprio territorio e sui propri cittadini richiede, per risolverla, più della semplice buona volontà[18].

Il primo punto da considerare è quel che si potrebbe definire l'atteggiamento mentale. L'idea dominante, per lungo tempo, è stata – come si è visto in apertura – che l'Internet, in quanto globale, è essenzialmente a-territoriale e può vivere grazie a regole auto-determinate. Dietro queste idea sembrano esserci diversi fraintendimenti.

a. Per dire le cose con una certa crudezza, nella prospettiva della sovranità, Internet non esiste. Esso è soltanto un protocollo per trasferire messaggi (pacchetti di dati) utilizzando reti pubbliche (*id est* aperte al pubblico) di telecomunicazioni. È chiaro che questo protocollo ha consistenza giuridica nel mondo della proprietà intellettuale e dal punto di vista regolamentare, ma essendo interamente non materiale esso non può formare oggetto di sovranità più di uno standard di telecomunicazione o di un sistema di misurazione metrico decimale. Non vi è sovranità sul protocollo Internet più di quanta ce ne possa essere sui protocolli utilizzati per i servizi Skype o WhatsApp.

b. Questo protocollo oggi esiste ed è utilizzato, ma nel futuro potrebbe essere sostituito da altre tecnologie o, molto semplicemente, alcuni Stati potrebbero decidere di usare standard delle comunicazioni su rete non compatibili con il protocollo Internet[19].

c. Il fatto che gli impulsi digitali che vengono trasmessi sono intangibili e vengono inviati grazie ad una entità non materiale (come il protocollo Internet) non significa in nessun modo che la rete sia immateriale. Essa, invece, è composta in larga misura da elementi fisici, collocati quasi interamente sul territorio sovrano dello Stato. L'unico caso di comunicazione extra-territoriale non-materiale è quella

il quale, dall'estero, abbia commesso atti dannosi «contro la infrastruttura digitale di un altro Stato». Il caso proposto nel testo, invece, è se coloro i quali operano attraverso Internet possono godere della protezione della legge di uno Stato, e se entità poste al di fuori del suo territorio possano essere tenuti al rispetto delle norme di un diverso Stato.

[18] Il rischio paventato è quello di una «Balcanizzazione dell'Internet in una molteplicità di sistemi chiusi protetti dall'accesso extra-territoriale di ISP situati all'estero» (J. Daskal, *The Un-Territoriality of Data*, cit. alla nt. 14, a p. 332). Simili preoccupazioni sono espresse A. Chander, U.P.LE, *Data Nationalism*, cit. alla nt. 10.

[19] Si tratta di una situazione comune nel passato: basti pensare alla vicenda, risalente agli anni '70 e '80 del secolo scorso con riguardo agli standards (fra loro incompatibili) per la televisione a colori (PAL, tedesco; e SECAM, francese).

di un messaggio proveniente da un satellite ricevibile direttamente dall'utente (ad es. con un telefono mobile satellitare) senza bisogno di una infrastruttura terrestre che lo distribuisca[20].

d. Gli Stati controllano i segmenti fisici delle rete di comunicazione e decidono quali standards vogliono accettare. Quindi sono gli Stati a decidere se vogliono ammettere, ed entro quali limiti, Internet sulle proprie reti. Internet non ha territorio – e dunque non pone questioni di sovranità – perché da un punto di vista tecnico non ne può avere uno: non 'possiede' (nel senso di controllare e comandare) cavi, satelliti, frequenze. Queste sono controllate dagli Stati, o altre entità sopra-nazionali le quali regoleranno Internet ed ogni altra tecnica digitale utilizzata per comunicare attraverso le reti, e tenderanno a farlo in maniera crescente[21].

5. I precedenti del mare, del cielo, dello spazio

Si dovrebbe, piuttosto, considerare che le reti di telecomunicazioni sono uno straordinario mezzo di comunicazione come lo è stato, fin dall'antichità, il mare e, dal XX secolo, lo sono il cielo e lo spazio[22].

[20] V. M. Mejia-Kaiser, *Space Law and Unauthorised Cyber Activities*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 349. Tuttavia – almeno con riguardo ad Internet – non si tratta della situazione ordinaria. L'equivoco ('L'errore fondamentale') è chiaramente evidenziato da I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 261 (a p. 266) disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016].

[21] V. P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt.15 : «Gli stati hanno la capacità di trasformare il ciber-spazio in un dominio sul quale possono esercitare la loro sovranità»(p.34).

[22] Già quasi 20 anni fa D.C. Menthe, in *Jurisdiction in Cyberspace: A Theory of International Spaces,* 4 *Mich. Telecomm. Tech. L. Rev.* 69 (1998) proponeva di qualificare il ciber-spazio come uno 'spazio internazionale' come l'Atartide, lo spazio extra-terrestre e l'alto mare. «Appare logico assimilarle all'alto mare, allo spazio aereo internazionale, allo spazio extra-terrestre»: W. Heintschel Von Heinegg, *Legal Implications etc.*, cit. alla nt. 7 , p.9; v. anche P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt.15 (p. 40 s.). La similitudine è utilizzata anche per stabilire la giurisdizione in questioni di diritto internazionale privato: v. W.Guillermo Jimenez, A.R. Lodder, *Analyzing Approaches*

La circostanza che nessuno fisicamente possieda le onde del mare, l'aria attraverso la quale volano gli aerei o sono trasmesse le onde radio, e che lo spazio extra-terrestre è al di fuori dell'ordinario controllo degli Stati non ha impedito lo sviluppo di regole comuni le quali consentono la cooperazione internazionale nelle attività marittime, aeree, di telecomunicazione e satellitari[23]. Anche in questi casi si è di fronte ad attività che originano da un paese e sono destinate ad altri paesi, spesso attraverso[24] o sopra altri paesi, o su territori internazionali[25].

Il contenuto di regole esistenti[26] o future comprende una varietà di

to Internet Jurisdiction Based on Model of Harbors and the High Seas, in 29 *Int'l R.Law, Computers & Techn.* 266 (2015).

[23] W. Heintschel Von Heinegg, *Legal Implications etc*, cit. alla nt.7 definisce il ciber-spazio come un «global common» ovvero una *res communis omnium* (a p.9); and K. Ziolkowsi, *General Principles of International Law as Applicable in Cyberspace*, cit. alla nt.9, a p.167 qualifica «Internet come un'altra risorsa condivisa globalmente, il ciber-spazio come un altro spazio comune. Si potrebbero nutrire dei dubbi in ordine a tali qualificazioni: è discutibile che cavi sottomarini o satelliti per telecomunicazioni possano definirsi una res communis e si dovrebbe distinguere chiaramente l'elemento nel quale operano (l'acqua, l'aria, lo spazio extra-terrestre), la infrastruttura fisica, e l'attività che attraverso la infrastruttura viene condotta». La stessa A. va oltre proponendo, *de lege ferenda*, che Internet sia considerato«patrimonio comune dell'umanità» (a p. 181). Contro la teoria dei «global commons» v. P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt.15 (pp. 14 ss.); B. Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, cit. alla nt.16, a p. 194 s. suggerisce che «una titolarità fiduciaria [*trusteeship*] potrebbe essere una soluzione più adeguata per il futuro» (*ibidem*).

[24] Questo pone nuove questioni. Com'è noto il percorso che una comunicazione Internet prende dipende da una serie di fattori che in generale prescindono dalla volontà del mittente. Si possono applicare le regole internazionali consuetudinarie sul transito? Possono gli Stati esercitare un diritto sovrano di controllare (ed eventualmente bloccare e 'sequestrare') le comunicazioni che passano attraverso il proprio territorio? W. Heintschel Von Heinegg, *Legal Implications etc*, cit. alla nt.7 propone che il transito potrebbe essere limitato sulla base di «regole consuetudinarie o convenzionali di diritto internazionale» (a p. 11). Per alcune possibili soluzioni tecnologiche onde evitare il transito attraverso determinati stati v. T. Maurer et al., *Technological Sovereignty*, cit. alla nt.2 (a p. 58f)..

[25] Una ovvia problematica è quella dei cavi sottomarini analizzata da W. Heintschel Von Heinegg, *Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables under International Law*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 291 disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016].

[26] Si discute fra gli studiosi di diritto internazionale se i tradizionali principi del diritto internazionale si applichino, e in che misura, al ciber-spazio. In senso affermativo v. K. Ziolkowsi, *General Principles of International Law as Applicable in Cyberspace*, cit. alla nt.9; E.T. Jensen, *Cyber Sovereignty: The Way Ahead*, 50 *Texas Int'l L.J.*. 275. Per una ulteriore ricognizione v. M.N. Schmitt, L. Vihul, *The Nature of International Law*

questioni: dagli standards tecnologici e la loro compatibilità alla identificazione dell'origine dei messaggi o lo stabilimento di coloro i quali forniscono servizi e contenuti.

Tuttavia la principale controversia – come risulta evidente dal caso *Schrems* – riguarda il contenuto di ciò che viene trasmesso attraverso le reti e quali attività possono, non possono e in quale maniera, essere svolte. Qualche indicazione potrebbe trarsi dal c.d. 'Internet Bill of Rights', ma questo copre solo una parte assai limitata di un quadro ben più ampio. Il governo di uno 'spazio' così grande come le reti globali richiede certamente l'individuazione e l'affermazione di diritti individuali[27], ma anche obblighi, doveri, norme dispositive, rimedi, regole per risolvere le controversie. Da questo punto di vista, da una prospettiva internazionale siamo ancora lontani da un assetto ancora embrionale.

La sentenza nel caso *Schrems* mette in luce l'esistenza di una controversia internazionale (chi controlla la rete e fissa le regole che governano le attività che vi si svolgono)[28] che può essere risolta solo attraverso i tipici strumenti del diritto internazionale[29].

Cyber Norms, Tallinn Paper n.5, CCD COE 2014 disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/Tallinn%20Paper%20No%20%205%20Schmitt%20and%20Vihul.pdf [ultimo accesso 10.7.2016].

[27] La prospettiva illustrata da M. Land, Toward an International Law of the Internet, 54 Harv. Int'l L. J. 393 (2013) fondata su una interpretazione espansiva dell'art.19 della Convenzione di New York del 1966 sui Diritti Civili e Politici appare influenzata da desiderata più che da una realistica (anche se rude) valutazione dell'attuale esercizio della sovranità degli stati sulle reti di telecomunicazione.

[28] Molte altre sono esposte da T. Maurer et al. , *Technological Sovereignty* , cit. alla nt.2 (a p. 63). Ad esse va aggiunta quella fra la Russia e la NATO sul diritto (ammesso che vi sia) applicabile alle c.d. ciber-guerre: v. A. Krutskikh, A. Streltsov, *International Law and the Problem of International Information Security*, in *International Affairs* n.6, 2014, 64 disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/International_Affairs_No6_2014_International_Law.pdf [ultimo accesso 10.7.2016]: «Alcuni esperti della NATO hanno sviluppato degli approcci per regolare scontri informatici (come il Tallinn Manual on the International Law Applicable to Cyber Warfare). La Russia segue una politica diametralmente opposta volta ad evitare scontri militari e politici nello spazio informatico» (a p. 75). E la risposta di W. Heintschel Von Heinegg, *International Law and International Information Security: A Response to Krutkikh and Streltsov*, Tallin Paper No.9, 2015 disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_09_2015.pdf [ultimo accesso 10.7.2016]

[29] V. P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt. 15 a p. 32. Nello stesso senso J. Daskal, *The Un-Territoriality of Data*, cit. alla nt.14 a p. .

6. Le sedi internazionali per il governo delle reti digitali

La sede naturale per discutere e fissare regole comuni sembrerebbe essere l'Unione Internazionale per le Telecomunicazioni (ITU/UIT) considerata la sua esperienza di oltre un secolo e mezzo (è stata fondata nel 1865) e la diretta competenza sulle tematiche delle comunicazioni trans-nazionali[30]. Inoltre l'ITU prevede espressamente che soggetti privati (come le industrie) giochino un ruolo nel processo normativo, un profilo particolarmente importante considerando che la maggior parte dei soggetti impegnati nella determinazione del protocollo Internet e dei protocolli Internet-compatibili sono privati[31].

L'ITU ha prodotto un certo numero di decisioni ed accordi che riguardano Internet, ma esclusivamente su aspetti tecnici[32]. Bisogna però aggiungere che gli atti costitutivi e fondamentali dell'ITU non contengono disposizioni e procedure che riguardino la risoluzione delle controversie, il che da un lato riduce significativamente la forza vincolante delle sue risoluzioni ma al tempo stesso consente ai suoi membri di trovare sistemi alternativi per risolvere le dispute fra loro e dare vigore alla regolamentazione[33].

[30] In questo senso v. I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 261 disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016].

[31] I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* cit. alla nt. 20 , a p. 271.

[32] I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* cit. alla nt. 20 a p. 264 evidenzia la complessità della distinzione fra regolazione tecnica di una infrastruttura e la regolazione dei contenuti di un servizio. Vi è tuttavia un notevole dibattito fra coloro che vorrebbero rafforzare il ruolo dell'ITU in questo campo, e quanti, come gli Stati Uniti e l'UE, hanno diversa visione (v. H. Tiirma-Klar, *Cyber Diplomacy: Agenda, Challenges and Mission*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 509, at p. 528 s.) disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016]. See also D. P. Fidler, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, in 17 *Insights*, Issue 6, Feb. 2013 [papers of the American Society of International Law], disponibile on-line alla pagina https://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision [ultimo accesso 10.7.2016].

[33] I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* cit. alla nt.20, a p. 276 : («Non vi è alcun meccanismo disponibile in caso di mancato rispetto». E' dubbio che l'alternativa sia il ricorso alla Corte Internazionale di Giustizia, suggerito da K. Ziolkowsi, *General Principles of International Law as Applicable*

L'occasione per un passo in questa direzione potrebbe essere rappresentati dai pendenti negoziati fra Unione Europea e Stati Uniti sul c.d. Trans-Atlantic Trade and Investment Partnership (TTIP)[34]. Alcuni commentatori hanno anche suggerito che la sentenza *Schrems* sarebbe un mezzo per rafforzare la posizione europea nel negoziare lo sviluppo dei servizi elettronici trans-atlantici i quali, comprensibilmente, sono uno dei principali impegni dell'amministrazione statunitense la quale apertamente sostiene le sue imprese in questo campo (Google, Apple, Facebook, Amazon etc.)[35].

in Cyberspace, cit. alla nt.9, a p. 175. Va peraltro osservato che nel caso di cavi sottomarini, regolati dalla Convenzione di Parigi del 1884 sulla Protezione dei cavi telegrafici sottomarini, e successivamente estesa alle comunicazioni telefoniche dalla Convenzione di Ginevra del 1958 sull'Alto Mare, le dispute potrebbero essere regolate sulla base delle Convenzione ONU del 1982 sul Diritto dei mari (v. W. Heintschel Von Heinegg, *Protecting Critical Submarine Cyber Infrastructure,* cit. alla nt.25 , a p. 308 s.).

[34] Per ragioni comprensibili la posizione dello US Trade Representative nel negoziato T-TIP è molto più chiaro su Internet v. https://ustr.gov/trade-agreements/free-trade-agreements/transatlantic-trade-and-investment-partnership-t-tip/t-tip-15 [ultimo accesso 10.7.2016]. La posizione dell'Unione si concentra di più sugli aspetti rispetto ai quali il divario con gli USA è meno forte, come nel caso del commercio elettronico v. http://trade.ec.europa.eu/doclib/docs/2015/january/tradoc_153009.pdf [ultimo accesso 10.7.2016].

[35] Nella misura in cui il negoziato TTIP si svolge nel generale quadro dell'OMC, una serie di elementi che sono stati delineati in quel contesto potrebbero essere opportunamente trasposti. V. I. Walden. *International Telecommunications Law, the Internet and the Regulation of Cyberspace,* cit. alla nt.20, alle pp. 278 ss (evidenziando, a p. 284 s., la maggiore efficacia delle procedure OMC per la risoluzione delle controversie). Opportunatamente parla di «market sovereignty» e di potenziali «market destroying measures» D.J.B. Svantesson, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on US Business,* 50 *Stan. J. Int'l L.*. 53 (2014). V. anche J.P. Trachchtman, *International Economic Law in the Cyber Arena*, in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, 373 disponibile on-line alla pagina https://ccdcoe.org/publications/books/Peacetime-Regime.pdf [ultimo accesso 10.7.2016]; nonché S.A.Aaronson, *Why Trade Agreements are Not Setting Information Free: The Lost History and Reinvigorated Debate Over Cross-Border Data Flows, Human Rights and National Security*, disponibile on-line alla pagina http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595809 [ultimo accesso 10.7.2016]; K. Eichensehr, *The Cyber-Law of Nations*, 103 *Geo. L.J.* 317 (2015) (sul ruolo dei soggetti privati nel governo di Internet).

7. Una visione d'insieme sulla 'sovranità digitale'

Il protocollo Intenet è una realtà non eludibile[36]. Evolverà tecnologicamente, economicamente, socialmente, trasformandosi in qualcosa di diverso, con un diverso nome. Ma concentrarsi esclusivamente su Internet rischia di guardare al problema da una prospettiva distorta. Le questioni attinenti alla sovranità forse, si spera, potranno trovare una soluzione guardando al quadro d'insieme, ed un approccio casuistico non è molto promettente: la protezione dei dati personali è intimamente connessa alle questioni di ciber-sicurezza; la tutela dei consumatori al commercio internazionale; le operazioni bancarie con la stabilità finanziaria; gli standards tecnologici con gli investimenti e il loro rendimento; l'applicazione della legge richiede indagini digitali transfrontaliere[37]. Il primo punto da individuare è individuare la sede dove negoziati seri possono essere iniziati; il secondo quello delle procedure da seguire nel processo decisionale[38]. Quindi si possono immaginare le varie tematiche, le quali sono tutte molto delicate da un punto di vista politico in quanto quasi tutte involgono i diritti dei singoli i quali utilizzano la messe di conoscenze e di opportunità offerte da Internet[39]. Da questo punto di vista si può osservare

[36] Non è questa la sede per analizzare i possibili sviluppi di Internet e le alternative, già esistenti, come il c.d. protocollo TOR (v. E.Çalışkan, T. Minárik, A-M Osula, *Technical and Legal Overview of the Tor Anonymity Network,* CCD COE, Tallinn 2015, disponibile on-line alla pagina https://cryptome.org/2015/07/TOR_Anonymity_Network.pdf [ultimo accesso 10.7.2016]. In ogni caso TOR è la dimostrazione che il protocollo Internet è solo uno dei tanti modi attraverso il quale è possibile accedere ed utilizzare una rete di telecomunicazione.

[37] Su quest'ultimo aspetto v. la Direttiva 41/2014 sull'Ordine europeo di indagine penale; nonchè il commento di A-M. Osula, *Accessing Extraterritorially Located Data: Options for States*, CCD COE – Nato Cooperative Cyber Defence Centre of Excellence, 2015 disponibile on-line alla pagina https://ccdcoe.org/sites/default/files/multimedia/pdf/Accessing%20extraterritorially%20located%20data%20options%20for%20States_Anna-Maria_Osula.pdf [ultimo accesso 10.7.2016]. V. inoltre l'art.32 della Convenzione di Budapest del 2001 sulla criminalità informatica.

[38] V. H. Tiirma-Klar, *Cyber Diplomacy: Agenda, Challenges and Mission*, e K. Ziolkowsi, *Confidence Building Measures for Cyberspace*, entrambi in K. Ziolkowsi (a cura di), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, alle pp. 509 e 533 disponibile on-line alla pagina https://ccdcoe.org/publications/books/PeacetimeRegime.pdf [ultimo accesso 10.7.2016].

[39] Gli Stati Uniti hanno chiaramente espresso la loro posizione sui molti aspetti qui analizzati nel documento ufficiale della Casa Bianca «Prosperity, Security, and Openness in a Networked World», May 2011 disponibile on-line alla pagina https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

che numerose regole comuni possono essere estrapolate dal documento dell'OCSE del 2014 «Principles for Internet Policy-Making» nel quale sono indicate le risposte a molti dei principali problemi che interessano i paesi sviluppati e che richiedono cooperazione internazionale[40]. Occorre tuttavia evitare il pericolo che il dibattito su queste tematiche sia condotto e diretto da minoranze estremamente rumorose che hanno eletto Internet nella loro terra-di-nessuno che sarebbe sottratta all'impero della legge[41]. Non solo non si può sfuggire alla millenaria saggezza dell'*ibi societas ibi ius* (e le reti di telecomunicazione sono una parte, molto importante, delle società contemporanee) ma, ancor più importante, occorre evitare di creare nuovi tabù (Internet è al di fuori del diritto) che favoriscono un fenomeno opposto: l'utilizzo da parte degli Stati di pratiche occulte, segrete se non illegali[42].

[ultimo accesso 10.7.2016]. E nel luglio 2011 il Department of Defense ha pubblicato un documento intitolato «Strategy for Operating in Cyberspace» disponibile on-line alla pagina http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [ultimo accesso 10.7.2016]; seguito, nel novembre 2011, dal «Cyberspace Policy Report» disponibile on-line alla pagina https://fas.org/irp/eprint/dod-cyber.pdf [ultimo accesso 10.7.2016].

[40] Disponibile on-line alla pagina http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf [ultimo accesso 10.7.2016] . L'indice elenca le seguenti questioni: «1.Promote and protect the global free flow of information. 2. Promote the open, distributed and interconnected nature of the Internet. 3. Promote investment and competition in high speed networks and services. 4. Promote and enable the cross-border delivery of services. 5. Encourage multi-stakeholder co-operation in policy development processes. 6. Foster voluntarily developed codes of conduct. 7. Develop capacities to bring publicly available, reliable data into the policy making process. 8. Ensure transparency, fair process, and accountability. 9. Strengthen consistency and effectiveness in privacy protection at a global level. 10. Maximise individual empowerment. 11. Promote creativity and innovation. 12. Limit Internet intermediary liability. 13. Encourage co-operation to promote Internet security. 14. Give appropriate priority to enforcement efforts». V. O. Pollicino, M. Bassini, *The Law of the Internet between Globalisation and Localisation*, in M. Maduro, K. Tuori, S. Sankari (a cura di), *Transnational Law: Rethinking European Law and Legal Thinking,* Cambridge UP*,* 2014, 346 (proponendo, a p. 372 s., il principio del mutuo riconoscimento).

[41] L'ovvio riferimento è al c.d. movimento «Anonymous» il quale opera sulla rete, spesso attraverso attacchi informatici nei confronti di coloro che individua come i propri avversari.

[42] Numerosi commentatori evidenziano che gli Stati hanno un interesse nel negare che le regole del diritto internazionale si applichino ad Internet: «Vi è una crescente evidenza che gli Stati si comportano come se vi fossero pochi, se non alcuno, limiti nello svolgimento di attività nel ciber-spazio» (P.A. Walker, *Law of the Horse to Law of the Submarine: The Future of State Behavior in Cyberspace*, in M. MAYBAUM, A-M. Osula, L. Lindstrom (a cura di), *7th International Conference on Cyber Conflict*, 2015 NATO

Abstract

The article analises the recent ECJ Schrems decision linking it to the 2014 Google Spain decision as an expression of EU sovereign powers on telecommunication networks. The article takes into account the various,competing, theories on 'sovereignty in cyber-space' pointing out ambiguities and misunderstandings (typically confusing the Internet protocol with an object of sovereign powers) and indicating the need for international cooperation in the appropriate fora (the ITU, the T-TIP negotiations) to set common rules which can enable free flow of communication and free provision of electronic services on transnational telecommunication networks.

CCD COE Publications at pp.97 and 104) (available on-line at https://ccdcoe.org/sites/default/files/multimedia/pdf/Art%2004%20Technological%20Sovereignity%20-%20Missing%20the%20Point.pdf [ultimo accesso 10.7.2016]. Analogamente v. P.W. Franzese, *Sovereignty in Cyberspace*, cit. alla nt.15 (a pp. 34 ss).

Giorgio Resta

La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE

Sommario: Introduzione. – 1. Le rivelazioni di Snowden e lo scandalo *NSA*. – 2. L'infrastruttura giuridica dei programmi di sorveglianza elettronica: il quadro costituzionale. – 3. (*Segue*): le regole di dettaglio. – 4. Il conflitto regolatorio USA/EU nella materia dei dati personali. – 5. La prospettiva della Corte di Giustizia: da *Digital Rights* a *Schrems*. – Conclusioni.

Introduzione

La decisione della Corte di Giustizia nel caso *Schrems c. Data Protection Commissioner* può essere considerata, se non un *leading case,* certamente uno dei precedenti più rilevanti nell'ambito della recente giurisprudenza europea in tema di diritti fondamentali. Per apprezzarne compiutamente il significato e le implicazioni, è necessario ricostruire, sia pure per grandi linee, il contesto politico e giuridico nel quale essa si inserisce. Su un piano 'micro' essa rappresenta l'ultimo tassello di un mosaico di pronunzie particolarmente innovative, tutte concernenti la tutela della riservatezza e dei dati personali, composto (per limitarsi alle principali)[1] dalle decisioni *Google Spain*[2]*, Digital Rights*[3] e per l'appunto *Schrems*[4]. Pur affrontando

[1] Ma per una disamina più dettagliata e completa si rinvia al contributo di G. Finocchiaro*, La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, *infra* in questo Volume.

[2] Corte di giustizia, *infra* 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/12; la decisione è pubblicata in *Dir. Inf.* 2014, 535, con molteplici commenti; v. anche G. Resta - V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

[3] Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources*, cause riunite C-293/12 e C-594/12, in *Dir. Inf.* 2014, 851, con nota di S. Scagliarini, *La Corte di Giustizia bilancia diritto alla vita privata e lotta alla criminalità: alcuni* pro *e alcuni* contra; e in *Nuova giur. civ. comm.,* 2014, I, 1044, con nota di C.M. Cascione, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione* data retention *della Corte di giustizia e gli echi del Datagate*.

[4] Corte di giustizia, Grande Sezione, 6 ottobre 2015, causa C-362/14, *Maximilian*

questioni diverse, ciascuna di esse offre un significativo contributo alla ridefinizione dello statuto dei dati personali nell'epoca dei *big data* e della 'sorveglianza liquida'[5]. Su un piano 'macro' essa costituisce uno specifico sviluppo del conflitto regolatorio, che ha diviso l'Unione Europea e gli Stati Uniti sin dall'entrata in vigore della direttiva 95/46/CE; conflitto che è deflagrato nel periodo 2013-2015, a seguito delle rivelazioni di Edward Snowden circa i programmi di sorveglianza di massa posti in atto dalle agenzie di informazione e sicurezza statunitensi (spesso in cooperazione con le omologhe agenzie europee)[6]. Offrire una lettura puramente 'interna' della pronunzia *Schrems*, che prescinda dalla considerazione di questi dati di contesto, rischierebbe di falsare i risultati dell'interpretazione. Queste pagine vorrebbero quindi soffermarsi piuttosto sulle premesse che non sulle implicazioni della decisione, guardando alla controversia *Schrems* come il prevedibile punto di sbocco di due principali situazioni di conflitto: da un lato quello, esogeno, tra il modello europeo e il modello statunitense di tutela della riservatezza; dall'altro quello, endogeno, tra le politiche della sicurezza e le garanzie costituzionali dei diritti di libertà.

1. Le rivelazioni di Snowden e lo scandalo NSA

Com'è noto, i documenti diffusi da Snowden e pubblicati dal *Guardian* e dal *Washington Post* nel giugno 2013 hanno disvelato i lineamenti essenziali dei programmi di sorveglianza di massa posti in essere dalle agenzie di *intelligence* statunitensi a seguito degli attacchi terroristici dell'11 settembre[7]. Si tratta di programmi che prevedono la raccolta su ampia scala

Schrems c. Data Protection Commissioner [Ireland], supra in questo Volume.

[5] Secondo la suggestiva formula di Z. Bauman – D. Lyon, *Liquid Surveillance,* Cambridge, 2012.

[6] In tema sia consentito rinviare a F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* 78 *Law & Cont. Prob's* 101 (2015); cfr. inoltre G. Sartor – M. Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU,* in *Dir. Inf.* 2014, 657.

[7] Per un quadro di sintesi v. C. Bowden, *The U.S. Surveillance Programmes And Their Impact On EU Citizens' Fundamental Rights* (2013), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf [ultimo accesso 12.7.2016]; sul problema dei rapporti con i programmi di sorveglianza europei v. D. Bigo et al., *National Programs for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law,* (2013), http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf

di informazioni e dati personali degli utenti di servizi di telecomunicazione statunitensi e stranieri. Tale raccolta e il successivo trattamento non avvengono in maniera mirata, secondo il modello tradizionale di «small data», ma rispondono in prevalenza alla logica dei *big data*: acquisizione su larga scala e in maniera automatica dei dati, conservazione per un lungo periodo di tempo, integrazione con altre banche dati e analisi attraverso potenti elaboratori elettronici dell'intero compendio informativo, con l'obiettivo di ricavarne inferenze statisticamente rilevanti per fini di «foreign intelligence»[8].

In particolare, le modalità principali di acquisizione di tali informazioni – secondo la configurazione originaria dei programmi in oggetto – sono due: *a*) l'intercettazione diretta del flusso di comunicazioni telefoniche e telematiche veicolato attraverso le reti statunitensi (programma UPSTREAM); *b*) l'accesso sistematico ai dati di traffico degli utenti, conservati nelle banche dati tenute dai maggiori fornitori di servizi di telecomunicazione e contenuti multimediali (quali Facebook, Google, Twitter, etc.) operanti negli USA (programma PRISM). Una volta acquisite, tali informazioni sono immesse in uno o più *database*, conservate per un ampio lasso temporale (generalmente 5 anni) e rese disponibili per ricerche mirate tramite appositi 'puntatori'[9]. Elementi connotativi di tali programmi sono: la segretezza (atteso che anche i provvedimenti giurisdizionali che autorizzano l'acquisizione presso terzi di dati e informazioni sono coperti dal vincolo di segreto)[10]; il carattere sistematico ed indiscriminato della raccolta (oggetto di raccolta e conservazione sono dati e metadati relativi a qualsiasi cittadino, indipendentemente dall'esistenza di indizi di reato)[11]; il raggio transfrontaliero delle operazioni di sorveglianza (interessati non sono soltanto i cittadini e i residenti sul territorio USA,

[ultimo accesso 12.7.2016].

[8] La differenza tra le tecniche di *small data* e *big data surveillance* è sintetizzata in maniera particolarmente nitida da M. Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, in 42 *Pepp. L. Rev.* 773 (2015).

[9] Per i dettagli tecnici v. D.S. Kris, *On the Bulk Collection of Tangible Things*, in 7 *J. Nat'l Security L. & Pol'y* 209 (2014); nonché C. Comella, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza «Safe Harbor» della Corte di giustizia dell'Unione Europea, infra* in questo Volume.

[10] IIn tema v. S. Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, in 51 *Stan. J Int'l L.* 69 (2015).

[11] M. Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, cit.; L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 *Harv. J.L. & Pub. Pol'y* 757 (2014).

ma anche gli stranieri)[12].

All'indomani della rivelazione dell'esistenza dei programmi di sorveglianza elettronica di massa, si è sviluppato negli Stati Uniti un ampio e articolato dibattito circa i limiti di legittimità e compatibilità democratica delle suddette attività. Rapporti di studio sono stati elaborati ad opera di diversi *think tank*, tra i quali su posizioni particolarmente critiche quello del *Brennan Center*[13], nonché di commissioni governative e parlamentari, tra le quali il *President's Review Group on Information and Communication Technologies*[14] e il *Privacy and Civil Liberties Oversight Board*[15]. Progetti di riforma sono stati presentati in Congresso e uno dei più importanti di essi, il US Freedom Act (*Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015*), approvato nel giugno 2015[16]. Lo stesso Presidente degli Stati Uniti ha disposto il mutamento delle procedure di *signal intelligence,* attraverso la *Presidential Policy Directive - PPD28* del Gennaio 2014[17]. Tuttavia, il tema al centro della discussione pubblica è stato, almeno sino a pochi mesi fa, quello della compatibilità dei sistemi di *bulk collection* dei dati personali con il quadro delle *American liberties,* ove il termine «American» sta ad indicare

[12] V. ad es. P. Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism,* 82 *Fordham L. Rev.* 2137 (2014).

[13] *What Went Wrong with the FISA Court*, Brennan Center for Justice at New York University School of Law (2015).

[14] President's Review Group on Information and Communication Technologies, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies Recommendation*, Recommendation 13, 12 dicembre 2013.

[15] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 luglio 2014.

[16] In base alla suddetta normativa, il programma di raccolta di massa di metadati telefonici da parte dell'NSA è d'ora in avanti abolito e sostituito da un meccanismo di *data retention* da parte dei providers di telecomunicazioni, ai quali le autorità competenti potranno rivolgersi per ottenere selettivamente l'accesso ai dati necessari per finalità di tutela della sicurezza nazionale; inoltre, si prevede che i destinatari di un ordine di esibizione dei metadati non siano vincolati ad un obbligo assoluto di non divulgazione e che i provvedimenti della FISC court siano soggetti, previo apposito filtro governativo, a un regime di pubblicità (per un'analisi dettagliata v. P. Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013,* Georgia Tech. Scheller College of Business Research Paper n. 36, December 18 2015, in http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2709619 [ultimo accesso 12.7.2016].

[17] Presidential Policy Directive - Signals Intelligence Activities, Jan. 17, 2014, accessibile all'indirizzo http:// www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [ultimo accesso 12.7.2016].

non soltanto il contenuto sostanziale delle libertà in oggetto[18], quanto soprattutto la nazionalità dei loro titolari. Infatti, l'attenzione dei cittadini, dei commentatori e dei giuristi, si è appuntata in maniera pressoché esclusiva sul problema della tutela dei diritti fondamentali dei cittadini statunitensi rispetto alle suddette pratiche di controllo di massa. Per contro, la questione della sfera privata degli stranieri è rimasta sullo sfondo, essendo destinata a riemergere soltanto quando le esigenze di 'normalizzazione' dei rapporti politici e soprattutto commerciali (in vista della finalizzazione delle negoziazioni per il TTIP) con l'Unione Europea hanno spinto all'approvazione del *Judicial Redress Act,* del quale si dirà meglio in seguito. Ciò, sia chiaro, era del tutto prevedibile, data la natura della posta in gioco e la delicatezza del tema del contrasto al terrorismo internazionale[19], oltre che la visione particolarmente 'insulare' che gli USA hanno sempre mantenuto sul tema del rispetto dei diritti umani. Una serie di interrogativi meritano però di essere sollevati, quanto meno per comprendere la natura e le implicazioni del conflitto sotteso alla decisione *Schrems*.

In base a quali presupposti le autorità federali hanno avuto accesso quotidianamente, per diversi anni, ad una mole immensa di dati relativi al traffico telefonico e Internet di cittadini (statunitensi e) stranieri? È ciò avvenuto in conformità o in violazione del quadro normativo interno o sovranazionale? Come affrontare nel futuro casi simili, indipendentemente dalle risposte che possano derivare dal quadro degli eventuali accordi bilaterali?

2. L'infrastruttura giuridica dei programmi di sorveglianza elettronica: il quadro costituzionale

Sembra si possa affermare, sulla scorta dei risultati ai quali sono pervenute diverse commissioni d'indagine, che il meccanismo di sorveglianza elettronica posto in essere dalle agenzie di sicurezza statunitensi non ha operato al di fuori dei circuiti della legalità, ma ha sfruttato alcune falle, o meglio alcune caratteristiche distintive, del regime statunitense di tutela

[18] Secondo l'accezione del sintagma fatta propria, ad esempio, da F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* in 48 *Bost. Coll. L. Rev.* 609 (2007).

[19] Cfr. F. Resta, *11 Settembre: attentato alle libertà? I diritti umani dopo le Torri Gemelle,* Roma, 2011.

della riservatezza[20]. Ferme restando alcune zone grigie di dubbia qualificazione, rispetto alle quali è tuttora aperto il contenzioso[21], il livello capillare di interferenza con la sfera privata non appare imputabile ad un abuso dei poteri pubblici (che potrebbe far pensare ad un nuovo *Watergate*), quanto piuttosto alle caratteristiche intrinseche del sistema normativo. L'architettura giuridica del sistema della sorveglianza elettronica post-11 settembre risulta, infatti, connotata da una notevole porosità e, specie là dove oggetto delle operazioni di intelligence siano le comunicazioni che coinvolgano almeno uno straniero, preordinata a una netta prevalenza del polo del controllo su quello della riservatezza. Ciò si evince non soltanto da un'analisi delle principali fonti in materia – il *Foreign Intelligence Surveillance Act*, il *Patriot Act* e l'*Executive Order* n. 12333 – ma anche del quadro delle regole costituzionali che di tali fonti rappresentano la griglia ordinante.

Prendendo le mosse proprio dal livello delle garanzie costituzionali, vi sono almeno tre elementi che meritano di essere segnalati, i quali riducono ad ambiti piuttosto ristretti il perimetro della tutela riconosciuta ai destinatari, e segnatamente agli stranieri, dei programmi di controllo.

In primo luogo sussiste una netta diversificazione del regime applicabile – ai sensi del Quarto Emendamento della Costituzione USA – alle interferenze con la sfera privata dettate, rispettivamente, da esigenze di contrasto della criminalità ordinaria e di protezione della sicurezza nazionale[22]. L'esistenza di un doppio binario è affermata dalla Corte Suprema sin dal celebre caso *United States v. United States District Court* (noto come Keith case)[23], nel quale si dibatteva dell'utilizzabilità di intercettazioni telefoniche disposte, senza previa autorizzazione dell'autorità giudiziaria,

[20] V. ad es. A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,* 21 *Mich. Telecomm. Tech. L. Rev.* 317, 358 (2015)

[21] Si veda in particolare la questione relativa alla compatibilità del programma di *bulk data collection* adottato ai sensi della Sect. 215 Patriot Act con il Quarto Emendamento: i casi più rilevanti in materia, i quali pervengono a conclusioni difformi, sono costituiti da *Obama v. Klayman,* 14-5004, U.S. Court of Appeals, District of Columbia Cir. (Aug. 2015); *Klayman v. Obama*, 957 F. Supp. 2d 1, 29 (D.D.C. 2013); *ACLU v. Clapper,* 14-42-cv, U.S. Court of Appeals, 2nd Cir. (May 2015); *ACLU v. Clapper*, F. Supp. 2d 724 (S.D.N.Y. 2013).

[22] F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* Bruxelles, 2015, 20; Id., *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* cit., 620-621.

[23] *United States v. United States District Court*, 407 U.S. 297 (1972).

nei confronti di alcuni membri del gruppo estremistico «White Panters», accusati di un attacco alla sede della CIA. La Corte ha tracciato una netta distinzione tra le intercettazioni disposte, da un lato, per finalità di prevenzione e repressione dei reati 'ordinari' e, dall'altro, per finalità di tutela della «sicurezza nazionale» [24]. Queste ultime troverebbero la loro legittimazione nella prerogativa costituzionale del Presidente di «preservare, proteggere e difendere la Costituzione degli Stati Uniti» e dovrebbero ritenersi preordinate a «proteggere il sistema costituito contro l'azione di coloro, i quali vorrebbero sovvertirlo o rimuoverlo attraverso mezzi illeciti». Tuttavia, 'sicurezza nazionale' è un concetto che la Corte circoscrive distinguendo due diverse ipotesi: *a*) la sicurezza nazionale nei suoi aspetti 'domestici' (protetta cioè nei confronti delle azioni eversive di gruppi interni); *b*) la sicurezza nazionale 'esterna' (rilevante nei confronti delle minacce provenienti da potenze straniere o da loro agenti). Le fattispecie rilevanti *sub a*), tra le quali il caso di specie, rientrerebbero nell'ambito oggettivo di applicazione del Quarto Emendamento, con la conseguente necessità del previo mandato giudiziario, assistito dal ragionevole sospetto della commissione di un reato. Le ipotesi rilevanti *sub b)* ne resterebbero fuori, non suscitando particolari preoccupazioni in termini di possibili abusi del potere esecutivo, a danno della libertà dell'espressione e del corretto funzionamento dei circuiti democratici[25]. Dunque, benché la Corte abbia lasciato aperto l'interrogativo concernente le eventuali salvaguardie da adottare nell'ambito delle operazioni di *foreign intelligence*, si è eliminato qualsiasi dubbio circa la duplicità del regime giuridico di riferimento, più garantistico nei casi di rischi per la *domestic security*; meno garantistico, invece, nei casi di minacce alla sicurezza nazionale provenienti dall'esterno.

In secondo luogo, l'ambito soggettivo di operatività del Quarto Emendamento risulta strutturalmente limitato per effetto della distinzione tra cittadini (ivi compresi i residenti permanenti) e stranieri. In particolare, sin dal caso *United States v. Verdugo-Urquidez*[26], recentemente richiamato in maniera adesiva in *Clapper v. Amnesty International USA*[27], la Corte Suprema ha affermato l'applicabilità del Quarto Emendamento a tutte le fattispecie di perquisizione e sequestro all'interno del territorio nazionale, indipendentemente dalla nazionalità dei soggetti coinvolti.

[24] L. Rush Atkinson, *The Fourth Amendment's National Security Exception: Its History and Limits,* 66 *Vand. L. Rev.* 1343, 1381 (2013).
[25] F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* cit., 20.
[26] *United States v. Verdugo-Urquidez*, 494 U.S. 1092 (1990).
[27] *Clapper v. Amnesty International USA*, 133 Sup. Ct. 1138, 1154 (2013).

Pertanto, si tratti di cittadini statunitensi, o di stranieri presenti a qualsiasi titolo sul suolo americano, le garanzie sancite dal Quarto Emendamento devono ritenersi comunque operanti. Per contro, qualora le ingerenze con la sfera privata si realizzino al di fuori del territorio nazionale, il Quarto Emendamento potrà essere invocato unicamente da quella «classe di persone che siano parte della comunità nazionale o che abbiano altrimenti sviluppato legami sufficienti con questo paese, tali da farle considerare parte integrante di tale comunità» [28]. Innestandosi all'interno del dibattito se la «costituzione segua la bandiera»[29], la questione dell'applicabilità extraterritoriale del diritto alla *privacy* (nei limiti della tutela offerta dal Quarto Emendamento) è stata dunque risolta dalla Corte nel senso più restrittivo[30]. Di conseguenza, mentre la cittadinanza è un criterio irrilevante ai fini del giudizio sulla legittimità di perquisizioni e sequestri condotti sul territorio USA, essendo tali atti comunque soggetti al rispetto dei vincoli costituzionali, essa opera come parametro identificativo della disciplina applicabile in tutte le ipotesi di azione extraterritoriale. Ne deriva che le intercettazioni condotte «al di fuori del territorio nazionale» ricadono nell'area di operatività del Quarto Emendamento unicamente nel caso in cui i soggetti coinvolti siano cittadini USA o a questi equiparabili. Per contro, qualora si tratti di stranieri, il Quarto Emendamento non sarebbe applicabile, in quanto norma strutturalmente preordinata alla tutela del popolo americano [31]. Ovviamente va chiarito, e sul punto si tornerà in seguito, in che modo si debba esattamente declinare la nozione di 'territorio' rispetto ad atti e rapporti condotti nella virtualità delle reti telematiche, e pertanto connotati da una specifica attitudine a-territoriale[32]. Resta fermo, comunque, che, pur soggetta a notevoli incertezze di ordine applicativo, tale diversificazione tra i regimi di tutela possiede un rilevante valore simbolico e di orientamento ermeneutico.

[28] *United States v. Verdugo-Urquidez*, cit., 265-268.

[29] K. Raustiala, *Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law*, Oxford, 2009.

[30] Per un'analisi approfondita di questi aspetti v. M. Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age,* in corso di pubblicazione in *Harv. Int. L.J.,* (2014) accessibile all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485 [ultimo accesso 12.7.2016].

[31] Tale regola di esclusione è rimarcata e difesa con argomenti non incontroversi da J. Yoo, *The Legality of National Security Agency's Bulk Data Surveillance Programs*, 37 *Harv. J. L. & Pub. Pol'y* 901, 919 (2014).

[32] Cfr. in tema J. Daskal, *The Un-Territoriality of Data*, di prossima pubblicazione in *Yale L.J.* (2015/16) e accessibile all'indirizzo http://insct.syr.edu/wp-content/uploads/2015/06/Daskal_Un-Territoriality_of_Data.pdf [ultimo accesso 12.7.2016].

In terzo luogo, il raggio applicativo del Quarto Emendamento si rivela alquanto ridotto anche sul piano oggettivo. Ciò è la conseguenza della ben nota *third-party doctrine*, fatta propria (e non ancora formalmente abbandonata) dalla Corte Suprema USA sin dai casi *United States v. Miller*[33] e *Smith v. Maryland*[34]. Essa verte sull'interpretazione della «reasonable expectation of privacy» quale coelemento della fattispecie di tutela della riservatezza ai sensi del Quarto Emendamento. Non vi sarebbe «reasonable expectation of privacy», ad avviso della Corte, qualora le informazioni in oggetto siano nella disponibilità di un terzo, che le ha originate o conservate in maniera strumentale al perseguimento di propri interessi, come nel caso della banca rispetto ai dati bancari e del fornitore di servizi di telecomunicazioni rispetto ai dati di traffico[35]. Ciò è coerente con il fondamentale asse «inside-outside», che struttura la logica statunitense tradizionale di tutela della riservatezza[36] e che induce alla conclusione che l'accesso da parte dei poteri pubblici alle informazioni volontariamente condivise con terzi non è subordinato agli stringenti requisiti posti dal Quarto Emendamento. Le ricadute di tale modello in ordine al problema della sorveglianza elettronica sono di immediata evidenza: l'acquisizione da parte delle autorità governative dei dati di traffico (ma non dei contenuti) in possesso dei fornitori dei servizi di telecomunicazione sarebbe sottratta al rispetto dei vincoli del mandato giudiziario e della *probable cause*[37].

3. (Segue): Le regole di dettaglio

Le premesse costituzionali appena illustrate appaiono oggi molto più controverse e meno univoche di quanto non fosse in passato. In particolare, la de-materializzazione dei rapporti indotta dalla sinergia tra digitalizzazione e interconnessione attraverso le reti telematiche ha revocato in dubbio molti dei presupposti fattuali sui quali si reggeva la lettura

[33] *United States v. Miller,* 425 U.S. 435, 443 (1976).
[34] *Smith v. Maryland*, 442 U.S. 735, 744–46 (1979).
[35] J.T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?,* in 74 *Fordham L. Rev.* 1731, 1743-1745 (2006).
[36] O.S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach,* in 62 *Stanford L. Rev.* 1005, 1009-1011 (2010).
[37] M. Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply,* in 54 *B.C.L. Rev.* 1, 12-17 (2013); F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* cit., 10.

tradizionale del Quarto Emendamento. Tra questi le dicotomie interno/esterno (sfera domestica di *privacy* / dati pubblici) e territorialità/extraterritorialità[38]. La recente controversia che ha contrapposto il governo USA e la società Microsoft, a proposito dell'ordine di esibizione di dati personali relativi a un soggetto privato e fisicamente archiviati in un server ubicato in Irlanda, ha evidenziato quanto siano labili i confini tra la nozione di accesso territoriale e accesso extraterritoriale nello spazio virtuale definito dalle reti telematiche[39]. Di qui le varie proposte di riforma avanzate in dottrina, tra cui quella, molto radicale, formulata da Orin Kerr e consistente nella sostituzione del criterio della nazionalità a quello della territorialità, come presupposto per l'applicazione del Quarto Emendamento[40]. Inoltre, la *third party doctrine* è stata fatta oggetto di numerose critiche, poiché inidonea a governare i nuovi fenomeni comunicativi dell'era digitale[41]. Alcune di queste critiche hanno peraltro trovato uno sbocco giudiziario, inducendo alcune corti ad affermare l'incompatibilità dei programmi di raccolta di massa dei dati di traffico con i principi costituzionali, e segnatamente con il Quarto Emendamento, interpretato in maniera più liberale rispetto alla risalente giurisprudenza della Corte Suprema[42]. Nonostante tali crepe siano profonde e verosimilmente destinate a espandersi, sta di fatto che gli equilibri definiti a livello costituzionale si sono fedelmente riprodotti anche sul piano delle regole di settore adottate negli anni '70 e profondamente rimaneggiate nel periodo successivo agli attacchi terroristici dell'11 settembre 2001[43].

Innanzitutto la disciplina dei programmi di sorveglianza per finalità di tutela della sicurezza nazionale segue fedelmente il doppio binario tracciato dalla Corte Suprema tra *law enforcement* e *foreign intelligence*.

[38] Sui due aspetti v. rispettivamente O.S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach,* cit.; O. S. Kerr, *The Fourth Amendment and the Global Internet,* 67 *Stan. L. Rev.* 285 (2015).

[39] *In re Microsoft*, 15 F. Supp. 3rd 466 (S.D.N.Y 2014).

[40] O. S. Kerr, *The Fourth Amendment and the Global Internet,* cit., 303-304.

[41] Tra i tanti v. M. Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply,* cit., spec. 50 ss.

[42] V. ad es. la decisione di primo grado nel caso *Klayman v. Obama*, 957 F. Supp. 2d 1, 29 (D.D.C. 2013); e, seppur fondata su argomenti diversi da quelli relativi alla costituzionalità del programma di intelligence, *ACLU v. Clapper,* 14-42-cv, U.S. Court of Appeals, 2nd Cir. (May 2015) (su cui M. Catanzariti, *ACLU v. Clapper: una nuova stagione per il right to privacy?,* in *Costituzionalismo.it,* n. 2/2015, http://www.costituzionalismo.it/articoli/526 [ultimo accesso 12.7.2016].

[43] Per un quadro di sintesi v. M. Nino, *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy,* in *Dir. umani e dir. int.*, 2013, 727, 733 ss.

Le due principali fonti normative in materia, ossia il *Foreign Intelligence Surveillance Act* (promulgato nel 1978, a seguito degli scandali emersi durante la presidenza Nixon)[44] e l'*Executive Order* 12333[45] (adottato dal Presidente Reagan nel 1981) si occupano esclusivamente della *foreign surveillance,* dettando un sistema di controllo che prescinde dalle garanzie iscritte nel Quarto Emendamento e dalle altre regole poste per la sorveglianza per finalità di *law enforcement* contenute nell'*Electronic Communications Privacy Act*[46]. Mette conto chiarire che la nozione di 'foreign' si articola diversamente nelle due ipotesi normative: la prima ha una connotazione soggettiva, in quanto copre prevalentemente le attività di sorveglianza mirate a soggetti stranieri, benché effettuate sul suolo americano; la seconda una connotazione oggettiva, in quanto pertiene alle attività di *intelligence* condotte all'estero[47].

In secondo luogo, la disciplina in esame riproduce e accentua il divario di tutela tra cittadini e stranieri fatto proprio dalla giurisprudenza costituzionale[48]. Le garanzie previste nel FISA appaiono essenzialmente preordinate, da un lato, a evitare che le attività di sorveglianza siano disposte per contrastare minacce puramente domestiche, rispetto alle quali rimane applicabile il sistema ordinario e, dall'altro, a far sì che la *privacy* e gli altri diritti fondamentali dei cittadini statunitensi accidentalmente caduti nella rete della sorveglianza siano adeguatamente tutelati. Ciò si ricava testualmente dal § 702 FISA[49], nella sua versione modificata a seguito del *Patriot Act*, ove si prevede che l'*Attorney General* e il *Director of National Intelligence* possono autorizzare la sorveglianza di persone «ragionevolmente ritenute al di fuori del territorio degli Stati Uniti al fine di acquisire *foreign intelligence information*». Tra le limitazioni espressamente previste si

[44] Per la ricostruzione storica v. L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 *Harv. J.L. & Pub. Pol'y* 757, 766-782 (2014).

[45] Per approfondimenti v. A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,* cit., 321 ss.

[46] In tema F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* cit., 626; A.K. Chhabra, *Fisa Surveillance and Aliens,* 82 *Fordham L. Rev. Res Gestae* 17, 23 (2014); M. Nino, *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy,* cit., 734.

[47] A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,* cit., 329-335.

[48] Sul punto v. A.K. Chhabra, *Fisa Surveillance and Aliens,* cit., 20; K. Lachmayer – N. Witzleb, *The Challenge to Privacy From Ever-Increasing State Surveillance: A Comparative Perspective,* 37 U.N.S.W. L.J. 748, 764 (2014).

[49] 50 U.S.C. § 1881a..

annoverano il divieto di sottoporre intenzionalmente a sorveglianza individui presenti al momento dell'acquisizione all'interno del territorio degli Stati Uniti, ovvero soggetti che si trovino al di fuori dei confini nazionali, ma siano «US persons» (cittadini e residenti permanenti); inoltre si prescrive l'adozione di procedure di «minimizzazione», con l'intento di evitare l'intercettazione delle comunicazioni relative a cittadini statunitensi e assicurare in ogni caso il rispetto dell'interesse alla *privacy* e alla libertà d'espressione di cui al Primo Emendamento[50]. Del pari, il secondo schema normativo di maggior rilevanza, quello delineato dal § 215 *Patriot Act*[51], contrappone nettamente il regime dell'acquisizione di *foreign intelligence information* concernente rispettivamente soggetti stranieri e cittadini americani. In quest'ultimo caso si prevede che l'ordine di esibizione (e segnatamente l'ordine di produrre «any tangible things») contemplato dalla norma in oggetto possa essere emesso soltanto nel quadro di investigazioni volte a contrastare il terrorismo internazionale o attività clandestine di spionaggio, sempre che ciò non avvenga esclusivamente sulla base di attività protette dal Primo Emendamento della Costituzione federale[52]. In entrambi i casi, quindi, la tutela accordata dal Primo Emendamento opera come un fattore conformativo della disciplina dell'attività di *intelligence* soltanto a beneficio dei soggetti di nazionalità statunitense, poiché si intende evitare che dietro lo schermo della tutela della sicurezza si celi un'attività repressiva del dissenso democratico[53]. Il rispetto della libertà di parola e di pensiero non vale, però, in questo contesto, a favore degli stranieri[54]. A ciò si aggiunga che – a differenza di quanto avviene nel sistema definito dalla direttiva 95/46/CE – la stessa normativa generale sul trattamento dei dati personali nel settore pubblico, il *Privacy Act* del 1974, si applica unicamente ai cittadini americani e agli stranieri ammessi con lo status di residente permanente[55]. Di riflesso le *non-US persons* sono normativamente collocate all'interno di uno spazio ben poco presidiato

[50] L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* cit., 791..
[51] 50 U.S.C. § 1861. In tema v. A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,* cit., 326; F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* cit., 24.
[52] L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* cit., 802.
[53] A.K. Chhabra, *Fisa Surveillance and Aliens*, cit., 20.
[54] A.K. Chhabra, *Fisa Surveillance and Aliens*, cit., 24.
[55] 5 U.S.C. § 552a (a) 2; sul punto v. F. Bignami, *The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens,* cit., 12..

sul piano dei meccanismi di garanzia e degli strumenti di tutela (i quali non sono completamente assenti, ma limitati a singoli settori, come quello presidiato dall'*Electronic Communications Privacy Act*[56]). Infine, l'interpretazione fornita dalla *Foreign Intelligence Surveillance Court* dei presupposti e del contenuto dell'ordine di esibizione previsto dal § 215 *Patriot Act* sembra confermare il regime di tutela affievolita per i metadati, implicito nella già illustrata *third-party doctrine*. Nel momento in cui la corte ritiene sufficiente emettere un unico provvedimento per legittimare una raccolta in massa e su base giornaliera di una mole elevatissima di dati, il controllo giudiziario preventivo – evocato varie volte dalle autorità statunitensi a testimonianza della sostanziale legittimità del programma di sorveglianza – viene di fatto ridotto ad un mero simulacro[57].

4. Il conflitto regolatorio USA/EU nella materia dei dati personali

Le onde d'urto del terremoto prodotto dalle rivelazioni di Snowden hanno innescato un processo di revisione dei meccanismi di controllo e sorveglianza elettronica, che potrebbe portare in futuro a mutamenti rilevanti. Tuttavia, come si è già accennato in precedenza, tale ripensamento critico ha interessato prevalentemente la questione della tutela dei cittadini statunitensi. Per quanto concerne la posizione degli stranieri, le uniche dichiarazioni di impegno sono state, almeno fino a pochi mesi fa, quelle riflesse nella *Presidential Policy Directive-PPD28*, le quali sembrerebbero peraltro ridimensionate degli orientamenti interpretativi sin qui adottati dalle autorità competenti[58]. Ciò ha determinato una tensione crescente con lo spazio giuridico e politico europeo, che è sfociata in un'aperta contrapposizione tanto sul piano parlamentare quanto su quello giurisdizionale[59].

Tale dinamica ha definito una nuova fase del conflitto regolatorio transatlantico, deflagrato a seguito dell'introduzione della direttiva 95/46/

[56] Cfr. *Suzlon Energy v. Microsoft Corporation*, 671 F.3d 726 (9th Circuit 2011).
[57] Così con argomenti molto persuasivi, L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* cit., 757 ss., 863-898.
[58] Si veda in proposito l'interessante analisi di D. Severson, *American Surveillance of Non-US Persons: Why New Privacy Protections Offer Only Cosmetic Changes,* in 56 *Harvard Int. L. J.* 465, 481-492 (2015).
[59] Sintetizzo qui quanto più approfonditamente esposto in F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* 78 *Law & Cont. Prob's* 101 (2015).

CE[60]. Difatti, ove se ne ripercorrano i momenti caratterizzanti, si potrà notare come in un primo momento il divario normativo USA/UE abbia prodotto attriti rilevanti soprattutto al livello del settore privato[61]. Era questo il contesto nel quale fu raggiunto, con notevoli difficoltà, l'accordo *Safe-Harbour*: difficoltà derivanti essenzialmente dalla diversa impostazione generale del sistema di tutela dei dati personali negli USA e in Europa. Mentre in Europa la disciplina si era sviluppata nel corso degli anni in maniera organica, includendo nel suo raggio d'applicazione tanto il settore pubblico quanto il settore privato e mirando a un bilanciamento (per quanto difficile e contestato) tra l'esigenza di libera circolazione dei dati nel mercato unico e quello della tutela dei diritti fondamentali, negli Stati Uniti il quadro rimaneva molto più asimmetrico e disorganico[62]. Il settore pubblico godeva di una regolamentazione tendenzialmente generale ed organica (il *Privacy Act*), la quale rispecchiava l'assunto condiviso negli anni '70 (l'epoca nella quale si erano diffusi i primi elaboratori elettronici di grandi dimensioni e limitata capacità di calcolo), per cui le minacce fondamentali alla sfera di riservatezza degli individui sarebbero derivate principalmente dal potere pubblico[63]. Per contro, il settore privato era connotato da discipline molto frammentarie (*cable communications act, video privacy act*, etc.), o dai rinvii alla potestà autoregolatoria dei privati (codici di condotta e simili), ove un ruolo fondamentale era giocato dal meccanismo del *notice and consent*[64]. La precomprensione del giurista, in questo caso, assegnava ai valori della libertà contrattuale, di iniziativa economica, nonché alla libertà d'espressione, un ruolo assiologicamente sovraordinato rispetto a quello della tutela (avvertita come paternalistica) del *data privacy*[65]. Si comprende quindi come la distanza più eclatante tra i due modelli regolatori si concentrasse sulla disciplina del trattamento dei dati in ambito privato, riducendosi tale divario nel settore pubblico a profili disciplinari importanti ma non decisivi (come l'assenza di un'autorità

[60] In tema si veda G. Sartor – M. Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU,* cit., 657 ss.
[61] J. Reidenberg, *E-Commerce and Trans-Atlantic Privacy,* in 38 *Hous. L. Rev.* 717, 728 (2001); F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* cit., 108-110.
[62] P.M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* in 126 *Harvard L. Rev.* 1966, 1974-1979 (2013).
[63] Cfr. in proposito P. Schwartz, *Data Processing and Government Administration: The Failure of the American Response to the Computer,* in 43 *Hastings L. J.* 1321 (1992).
[64] J. Reidenberg, *E-Commerce and Trans-Atlantic Privacy,* cit., 725-730.
[65] In termini generali v. J.Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty,* 113 *Yale L. J.* 1151 (2004).

amministrativa indipendente, il limitato rilievo del principio di necessità/*data minimization*, o il meccanismo di *enforcement* incentrato sull'iniziativa dei privati e sui rimedi risarcitori) [66]. Di qui la via dei *Safe Harbor Privacy Principles*, che avrebbero dovuto risolvere tale conflitto in una maniera *market-friendly*[67], e di qui anche la fragilità delle garanzie previste nello stesso Accordo per l'ipotesi di accesso da parte del settore pubblico ai dati detenuti da soggetti privati (vedi *infra,* § 6).

Nella sua prima fase di applicazione, il meccanismo di coordinamento sembrava avere dato buona prova di sé: l'adesione volontaria al sistema *Safe Harbor* da parte di alcune delle più importanti aziende statunitensi, insieme all'innalzamento dello standard di tutela a favore di tutti gli utenti (europei e non) e al ruolo di supervisione assunto dalla Federal Trade Commission, aveva fatto parlare di una competizione al rialzo, elevando la materia della protezione dei dati a controprova empirica del fenomeno descritto dagli scienziati della politica come *Brussels effect*[68]. Le rivelazioni di Snowden hanno gettato una diversa luce sul meccanismo in esame, facendo emergere gli elementi di criticità insiti nel fenomeno dell'accesso sistematico da parte dei poteri pubblici ai dati di terzi detenuti in mano privata: i dati legittimamente acquisiti nell'ambito dei rapporti contrattuali con soggetti privati (e trasferiti all'estero conformemente alle procedure *Safe Harbor*) vengono poi fatti oggetto di acquisizione in blocco e trattamento da parte di autorità pubbliche al di fuori di un adeguato quadro di garanzie e diritti. Questo, fondamentalmente, è il problema operativo da cui ha origine la controversia *Schrems*, la quale però non rappresenta il primo momento di emersione del suddetto conflitto e si inserisce all'interno di una più ampia dialettica tra sistema europeo e sistema statunitense. Difatti, l'Accordo *Safe Harbor* rappresentava il momento terminale di una prima forma di attrito tra i due ordinamenti, relativa soprattutto alla disciplina del settore privato e dei rapporti di mercato. All'indomani dell'11 settembre e dell'introduzione di una capillare normativa antiterrorismo negli USA, la quale ha notevolmente compresso i già non amplissimi spazi di protezione della *privacy* informativa, il suddetto conflitto regolatorio si

[66] La più approfondita analisi comparatistica è quella offerta da F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,* cit., 619-635.

[67] P.M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures,* cit., 1979 ss.; J. Reidenberg, *E-Commerce and Trans-Atlantic Privacy,* cit., 738 ss.; in tema si veda anche il contributo di V. D'Antonio – S. Sica, *I* Safe Harbor Privacy Principles*: genesi, contenuti, criticità, infra* in questo Volume.

[68] A. Bradford, *The Brussels Effect,* 107 *N.W. U. L. Rev.* 1, 22-26 (2012).

è progressivamente spostato dal settore privato al settore pubblico[69]. La prima disputa rilevante in ordine cronologico ebbe origine dalla pretesa da parte delle autorità USA di ottenere preventivamente da parte delle compagnie aeree la comunicazione dei dati identificativi dei passeggeri di voli per, da o attraverso gli Stati Uniti[70]. Investita della questione da parte delle stesse compagnie, la Commissione ha negoziato un accordo con il governo USA volto ad assicurare un quadro minimo di tutele, incentrato sui principi di trasparenza, accuratezza e sicurezza (originariamente siglato nel 2004, poi rinnovato nel 2007 e nel 2012) [71]. La seconda occasione di conflitto fu rappresentata dall'acquisizione coattiva da parte del Dipartimento del Tesoro USA, in attuazione del *Terrorist Finance Tracking Program* (TFTP), di una vasta messe di dati finanziari concernenti trasferimenti di fondi e altre operazioni bancarie da parte della *Society for Worldwide Interbank Financial Telecommunications* (SWIFT), la cui sede principale è ubicata in Belgio, ma con succursali operative anche in Olanda e negli USA[72]. La controversia che ne è derivata ha condotto infine all'approvazione nel 2010 di un apposito accordo bilaterale (TFTP II), che introduce specifiche salvaguardie per i dati personali relativi a cittadini europei[73].

5. La prospettiva della Corte di Giustizia: da Digital Rights *a* Schrems

Il c.d. Datagate rappresenta quindi soltanto l'ultimo capitolo di una dinamica di confronto più ampia, la quale però aveva visto sin qui pro-

[69] F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation,* cit., 110-117.

[70] In tema M. Botta – M. Viola de Azevedo Cunha, *La protezione dei dati personali nelle relazioni tra UE e USA, le negoziazioni sul trasferimento dei PNR,* in *Dir. Inf.* 2010, 315.

[71] Decisione della Commissione 2004/535, 2004 O.J. (L 235) 11; Agreement between the European Union and the United States of America on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS), 2007 O.J. (L 204) 18; Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security, 2012 O.J. (L 215) 5.

[72] Si veda F. Clementi – G. Tiberi, *Sicurezza interna, diritti e cooperazione internazionale nella lotta al terrorismo: i casi Pnr e Swift,* in www.astrid-online.it, 2013.

[73] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, 2010 OJ (L 195) 5.

tagonista la Commissione europea e in una posizione alquanto defilata la Corte di Giustizia. Il cambiamento del quadro istituzionale determinato dal Trattato di Lisbona, e in particolare l'attribuzione alla Carta dei Diritti di un'immediata efficacia precettiva e del medesimo valore giuridico dei Trattati, ha contribuito ad alterare un siffatto equilibrio[74]. La Corte di Giustizia sembra avere assunto una posizione notevolmente più incisiva e coraggiosa, non diversamente peraltro dal Parlamento Europeo, che ha risposto allo scandalo NSA con molteplici iniziative, tra le quali l'approvazione di uno specifico emendamento alla Proposta di Regolamento Generale sulla tutela dei dati personali volto a imporre la mediazione istituzionale delle autorità di garanzia europee per i casi di trattamento dei dati per finalità di giustizia da parte delle autorità straniere (c.d. *anti-PRISM clause*) [75]. Nelle tre decisioni ricordate in apertura del presente scritto – *Google Spain, Digital Rights* e *Schrems* – la Corte ha ribadito il rango primario del diritto alla protezione dei dati, traendone una serie di

[74] In generale su questi aspetti v. F. Bestagno, *I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia,* in *Dir. umani e dir. int.,* 2015, 259, spec. 262, 266 ss.

[75] Questo il testo dell'art. 43a nella sua proposta originaria: «1.No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State. 2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority. 3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with Article 44(1)(d) and (e) and (5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57. 4. The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1)». Nel testo definitivo del Regolamento la norma è stata così modificata: «Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter».

implicazioni particolarmente significative sia sul piano della circolazione transfrontaliera dei dati, sia su quello del bilanciamento con i legittimi interessi alla sicurezza nazionale e alla libertà d'impresa[76].

In *Google Spain* la Corte ha proposto una lettura a compasso allargato della clausola di giurisdizione iscritta nell'art. 4 della direttiva 95/46/CE, forzando interpretativamente la formula «contesto delle attività di uno stabilimento»[77], così da sovrapporla al criterio dell' «offerta di beni e servizi indirizzata a soggetti dell'Unione», fatta propria da diversi atti del diritto privato regolatorio[78], nonché dal nuovo Regolamento Generale sulla tutela dei dati personali (art. 3, comma 2, lett. a) [79]. In tal modo il perimetro di operatività della disciplina europea in materia di protezione dei dati personali risulta notevolmente ampliato, tanto da far parlare di una vera e propria applicazione extra-territoriale della normativa comunitaria[80]. L'obiettivo sotteso a un siffatto intervento, come pure al Regolamento, consiste verosimilmente nel contrasto alle strategie di aggiramento della disciplina di protezione, funzionale peraltro anche all'attuazione di condizioni di parità concorrenziale per tutti gli operatori che si rivolgono al mercato europeo[81]. Appare giustificato, a tal riguardo, parlare di un vero e

[76] I In tema si leggano i contributi di G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, e di O. Pollicino – M. Bassini, *La Carta dei dritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, entrambi *infra* in questo Volume..

[77] Sull'art. 4 della direttiva e i criteri di giurisdizione ivi fissati cfr. L. Moerel, *The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU citizens by Websites Worldwide?, Int'l Data Privacy L.,* 2010, 1.

[78] H.W. Micklitz, *The Internal v. The External Dimension of European Private Law – A Conceptual Design and a Research Agenda,* EUI Working Papers, 2015, 7, accessibile all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2627718 [ultimo accesso 12.7.2016].

[79] IIn tema v. G. Caggiano, *L'interpretazione del 'contesto delle attività di stabilimento' dei responsabili del trattamento dei dati personali,* in *Dir. Inf.* 2014, 616-618; e in G. Resta – V. Zeno-Zencovich, a cura di, *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* Roma, 2015, 55; P. Piroddi, *Profili internazionalprivatistici della responsabilità di un motere di ricerca per il trattamento dei dati personali,* in *Dir. Inf.* 2014, 623 ss.; G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da* Google Spain *a* Schrems, *infra* in questo Volume. Nell'ambito della giurisprudenza della Corte di Giustizia cfr. anche la sentenza del 1° ottobre 2015, causa C-230/14, *Weltimmo*.

[80] B. van Alsenoy – M. Koekkoek, *Internet and jurisdiction after* Google Spain*: the extraterritorial reach of the 'right to be delisted',* 5 *Int'l Data Privacy L.* 105, 110-111 (2015)..

[81] In questa prospettiva cfr. anche G. Sartor – M. Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU,* cit., 674-678; per una disamina delle implicazioni della decisione *Google Spain* in ordine al flusso transfrontaliero dei dati v. M.L. Rustad – S. Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data*

proprio atto di esercizio della 'sovranità digitale' [82].

Con la decisione *Digital Rights* l'asse dell'intervento giurisdizionale si appunta invece sul settore pubblico e segnatamente sul conflitto tra *privacy* e sicurezza[83]. Investita della questione concernente la validità della direttiva 2006/24/CE, la Corte rileva che l'obbligo di conservazione dei dati di traffico per un periodo compreso tra 6 mesi e 2 anni integra un'ingerenza illecita nella sfera di riservatezza tutelata dagli artt. 7 e 8 della Carta dei Diritti. In particolare, la Corte osserva che, pur non essendo violato il contenuto essenziale dei suddetti diritti *ex* art. 52, par. 1, della Carta (essendo escluso l'accesso al contenuto delle comunicazioni e essendo previste alcune garanzie minime di protezione dei dati personali) [84], la normativa comunitaria comporta un sacrificio sproporzionato dei diritti alla riservatezza e alla tutela dei dati personali sotto tre profili fondamentali: *a*) il carattere generale e indifferenziato del programma di conservazione dei dati, e dunque l'assenza di limiti nella fase della raccolta; *b*) la durata irragionevole del periodo di conservazione; *c)* l'assenza di idonee garanzie in punto di accesso da parte dei terzi e utilizzo dei dati. In sostanza la Corte rigetta le tecniche di *blanket data retention,* in quanto idonee a determinare nei cittadini la sensazione che 'la loro vita privata sia oggetto di costante sorveglianza' [85] e quindi – anche a prescindere dall'esistenza di uno specifico pregiudizio (richiesto invece dalla Corte Suprema USA quale prerequisito dello *standing* nei casi in cui si censuri la legittimità dei programmi di sorveglianza elettronica)[86] – incompatibili con i valori di dignità e autodeterminazione informativa accolti dall'ordinamento europeo[87]. Ciò giustifica la soluzione particolarmente rigorosa adottata dalla Corte, la quale sancisce, per la prima volta, l'invalidità totale di una direttiva

Flow, 28 *Harvard J. L. & Tech.* 349 (2015).

[82] V. Zeno-Zencovich, *Intorno alla decisione nel caso* Schrems*: la sovranità digitale e il governo internazionale delle reti di telecomunicazione, retro* in questo Volume.

[83] In tema M. Nino, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di* data retention, in *Dir. Un. Eur.,* 2014, 803, spec. 806 ss.

[84] Corte di giustizia, 8 aprile 2014, cit., §§ 39-40; sul punto v. O. Pollicino – M. Bassini, *La Carta dei dritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, cit., par. 5.

[85] Corte di giustizia, 8 aprile 2014, cit., § 37.

[86] *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013); sul punto v. le considerazioni critiche di N.M. Richards, *The Dangers of Surveillance,* 126 *Harv. L. Rev.* 1934, 1935 (2013).

[87] Si veda nella medesima prospettiva la decisione Corte eur. Dir. uomo, 4 dicembre 2008, nn. 30562/04 e 30566/04, *S. and Marper v. UK.*

del Parlamento e del Consiglio per contrasto con la Carta dei Diritti[88].

Il monito espresso dalla Corte si indirizzava principalmente nei confronti dei governi europei, fautori negli ultimi anni di una politica che, in nome all'interesse alla sicurezza, aveva legittimato restrizioni sempre maggiori della sfera dei diritti fondamentali dei cittadini, delle quali la direttiva 2006/24/CE costituiva un esempio emblematico[89]. Tuttavia l'apparato argomentativo della decisione lasciava chiaramente intendere che analoghi, se non più incisivi, strumenti di salvaguardia avrebbero dovuto essere apprestati per l'ipotesi in cui la raccolta e la conservazione dei dati fossero disposti, per le medesime ragioni di sicurezza, da parte di autorità straniere. Ciò si desume in maniera inequivocabile dal § 68 della pronunzia, ove si legge che «tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, e di conseguenza non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta, del rispetto dei requisiti di protezione e di sicurezza, quali richiamati ai due punti precedenti. Orbene, siffatto controllo, effettuato in base al diritto dell'Unione, costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali» [90]. È difficile non cogliere in filigrana un riferimento sufficientemente preciso al fenomeno – già di dominio pubblico al momento della decisione – dell'accesso sistematico da parte delle autorità USA ai dati personali relativi a cittadini europei.

Vista in quest'ottica, la decisione *Schrems* non fa che trarre le logiche conseguenze dalle premesse fissate nella pronunzia *Digital Rights* e segnatamente dal tipo di bilanciamento ivi accolto tra *privacy* e sicurezza. Oltre a negare l'effetto preclusivo del giudizio di adeguatezza compiuto dalla Commissione ex art. 25 nei confronti delle autorità di protezione dei dati nazionali[91], la Corte si spinge a sindacare nel merito la validità della Decisione 2000/520 della Commissione, travalicando i confini posti dalla domanda di rinvio pregiudiziale. Significativo è innanzitutto il modo in cui tale sindacato è condotto, in quanto la Corte appunta la propria attenzione non tanto sul contenuto intrinseco dei Principi stabiliti nell'Accordo *Safe Harbor* (i quali vincolano in primo luogo i soggetti *privati*

[88] Sul punto v. F. Bestagno, *I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia,* cit., 266.
[89] Per un quadro di sintesi v. l'ampia indagine di M. Nino, *Terrorismo internazionale, privacy e protezione dei dati personali,* Napoli, 2012, 147-350.
[90] Corte di giustizia, 8 aprile 2014, cit., § 68.
[91] Corte di giustizia, 6 ottobre 2015, cit., §§ 38-66.

che aderiscano al programma di autocertificazione) [92], quanto sul quadro istituzionale dell'ordinamento con il quale tali Principi sono destinati a interagire. L'anello critico dell'intero sistema è costituito dalla clausola – di cui all'Allegato I, quarto comma della Decisione – con la quale si stabilisce che l'applicabilità dei Principi in esame può essere limitata «se e inquanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]» [93]. Questa clausola rende possibili – come osservato dalla Corte – ingerenze, fondate su esigenze connesse alla sicurezza nazionale, nei diritti fondamentali dei cittadini europei[94]. È per il suo tramite, infatti, che le autorità USA hanno potuto acquisire in maniera formalmente legittima una massa enorme di dati personali relativi a cittadini europei, trasferiti dai providers di telecomunicazioni in osservanza dei principi *Safe Harbor*. Ne deriva un duplice ordine di questioni: *a*) sussistono nell'ordinamento di destinazione regole idonee a limitare le suddette ingerenze allo stretto necessario per conseguire il legittimo obiettivo della protezione della sicurezza nazionale?; *b*) sono previsti specifici rimedi, di natura giurisdizionale o amministrativa, a tutela dei soggetti destinatari dei programmi di sorveglianza? Tali quesiti sono rilevanti ai fini del giudizio di adeguatezza di cui all'art. 25 della Direttiva, interpretato alla luce della Carta dei Diritti Fondamentali dell'Unione Europea[95]. A ciascuno di essi la Corte dà una risposta negativa. Attribuendo uno specifico rilievo alle risultanze empiriche dell'indagine condotta dalla Commissione bilaterale UE/USA, la Corte stigmatizza tanto l'estensione e i caratteri dei programmi di *bulk collection* adottati dalle agenzie statunitensi, quanto l'assenza di alcun rimedio esperibile da parte dei cittadini europei[96]. In particolare, viene giudicata radicalmente incompatibile con i precetti di cui agli artt. 7 e 8 della Carta dei Diritti una normativa, quale quella statunitense, «che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare

[92] Corte di giustizia, 6 ottobre 2015, cit., § 98.
[93] In tema cfr. anche V. D'Antonio – S. Sica, I Safe Harbor Privacy Principles: *genesi, contenuti, criticità*, cit., par. 3.4.
[94] Corte di giustizia, 6 ottobre 2015, cit., § 87.
[95] Su questo modello interpretativo v. in particolare F. Bestagno, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali, in Il dir. dell'Un. Eur.*, 2015, p. 25 ss.
[96] Corte di giustizia, 6 ottobre 2015, cit., § 90 ss.

l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta» [97]. Tali ingerenze vanno ben oltre quanto strettamente necessario ai fini della protezione degli obiettivi di interesse pubblico (ledendo pertanto il principio di proporzionalità) e, nel caso specifico del diritto al rispetto della vita privata (art. 7 Carta), ne intaccano il contenuto essenziale, sottoponendo lo stesso contenuto delle comunicazioni ad un regime di tutela particolarmente affievolito[98]. Inoltre risulta leso il contenuto essenziale del diritto a una tutela giurisdizionale effettiva (art. 47 Carta), per ciò che al singolo individuo è negata sia la facoltà di accedere ai dati che lo riguardano, sia di ottenere la rettifica o la soppressione di tali dati[99]. Di qui la declaratoria di invalidità della Decisione 2000/520, in quanto atto interno idoneo a legittimare, sia pure in via mediata, la compressione dei diritti fondamentali dei cittadini europei da parte delle autorità estere.

Conclusioni

A seguito della controversia *Schrems c. Data Protection Commissioner* l'attitudine 'extraterritoriale' della normativa europea in materia di protezione dei dati risulta ulteriormente rafforzata[100]. Se con la pronunzia *Google Spain* l'ambito oggettivo di applicazione della direttiva definito dall'art. 4 è stato esteso in via interpretativa, con la decisione *Schrems* è lo strumento offerto dall'art. 25 a essere significativamente potenziato. Tali interventi s'iscrivono con coerenza all'interno della dinamica di competizione regolatoria descritta in precedenza, dove ai ripetuti fenomeni di violazione transfrontaliera dei diritti fondamentali – resi possibili dallo sviluppo delle tecnologie dell'informazione e della comunicazione – corrispondono pun-

[97] Corte di giustizia, 6 ottobre 2015, cit., § 93.
[98] Corte di giustizia, 6 ottobre 2015, cit., § 94; sul punto si leggano le considerazioni di O. Pollicino – M. Bassini, *La Carta dei dritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, cit.
[99] Corte di giustizia, 6 ottobre 2015, cit., § 95.
[100] In generale v. Dan J.B. Svantesson, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses,* 50 *Stan. J. Int'l L.* 53, 71 (2014); Id., *Extraterritoriality in the Context of Data Privacy Regulation,* 7 *Masaryk Univ. J. L. & Tech.* 87 (2013); più articolato il quadro argomentativo offerto da Y. Poullet, *Transborder Data Flows and Extraterritoriality: The European Position,* 2 *J. Int'l Commerc. L. & Tech.* 146 (2007).

tualmente meccanismi di reazione a carattere dichiaratamente 'nazionalistico'[101]. Tale termine non è impiegato in un'accezione dispregiativa, bensì per denotare l'impronta tipicamente 'locale' del modello di disciplina (e di bilanciamento degli interessi) che si intende proteggere, a fronte dei rischi di aggiramento derivanti dall'utilizzo delle tecnologie informatiche e dalla de-localizzazione dei dati su server remoti[102]. Tali reazioni possono essere di varia natura: la proposta avanzata in Francia e in Germania di dare vita ad un *cloud* europeo costituisce una tipica risposta a carattere tecnologico, che preluderebbe a nuove forme di autarchia digitale[103]; mentre gli interventi della Corte di Giustizia fanno ricorso, piuttosto che agli arcani ingranaggi del 'codice' tecnologico, alla 'mano visibile' della legge. Ciò non toglie che in entrambi i casi l'obiettivo di fondo consiste nella riaffermazione della sovranità del sistema di riferimento, declinata nel senso più specifico della sovranità digitale[104], a dispetto di tutte le tesi anarco-libertarie affermate nella prima fase dello sviluppo dell'Internet, le quali rivendicavano, in uno con l''aterritorialità' dei rapporti digitali, la loro strutturale immunità dalla potestà regolatoria degli Stati[105]. Poste queste premesse, è ragionevole ipotizzare che la dialettica transatlantica prosegua secondo il consueto itinerario, sostituendo alla fase dell'aperto confronto quella della negoziazione tesa a nuovi accordi bilaterali[106].

In effetti, l'osservazione degli ultimi sviluppi delle relazioni USA/UE sembra muoversi esattamente in questa direzione. Da un lato le negoziazioni tra le autorità europee e quelle statunitensi hanno condotto alla stipula del nuovo Accordo «Privacy Shield» , il quale sostituisce il precedente Safe Harbor[107]. Dall'altro il Congresso degli Stati Uniti ha approvato, nel

[101] A. Chander – U.P. Lê, *Data Nationalism, 64 Emory L.J. 677* (2015).
[102] V. Zeno-Zencovich, *Intorno alla decisione nel caso* Schrems*: la sovranità digitale e il governo internazionale delle reti di telecomunicazione,* cit.
[103] A. Chander – U.P. Lê, *Data Nationalism*, cit., 690-692.
[104] V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo Internazionale delle reti di telecomunicazione*, cit., par. 2.
[105] Per una ricostruzione attenta di tali tesi, ed una discussione della famosa 'Dichiarazione d'indipendenza del Cyberspazio' di J.P. Barlow, si veda R.H. Weber, *Realizing a New Global Cyberspace Framework. Normative Foundations and Guiding Principles,* Berlin-Heidelberg, 2014, 15 ss.
[106] PPer alcune considerazioni in proposito v. M. Nino, *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy,* cit., 743.
[107] Per un'analisi dettagliata dei contenuti dell'accordo v. T. Grau – T. Granetzny, *EU-US-Privacy Shield – Wie sieht die Zukunft des transatlantischen Datenverkehrs aus?,* in *NZA,* 2016, 405 ss.; S. Sica – V. D'Antonio, *Verso il Privacy Shield: il tramonto dei Safe Harbor Privacy Principles, infra* in questo Volume.

dicembre 2015, il *Judicial Redress Act.* Tale legge estende alcune delle (già deboli) garanzie di tutela dei dati personali, riconosciute in capo ai cittadini statunitensi dal *Privacy Act* del 1974, e segnatamente la possibilità di agire per il risarcimento dei danni arrecati per il trattamento illecito di tali dati da parte delle agenzie governative, ai cittadini dei «covered countries» (ossia i paesi o le organizzazioni regionali selettivamente riconosciuti dall'Attorney General), venendo incontro quindi ad una parte delle richieste avanzate dalle autorità europee[108].

Il problema della tutela degli stranieri viene dunque affrontato secondo la più classica delle logiche 'bilaterali'. L'indispensabile esercizio di realismo non deve, però, fare perdere di vista la peculiarità degli interessi coinvolti nel campo della tutela dei dati personali, i quali trascendono il paradigma tradizionale della sovranità territoriale per attingere alla dimensione tipicamente universalistica dei diritti umani. Riguardata unicamente nell'ottica della competizione regolatoria (che pure assume, come si è visto, un peso rilevante), la vicenda *Schrems* potrebbe essere liquidata come una peculiare riaffermazione del *soft power* europeo, ove si demanda alla logica dei diritti ciò che non si riesce a conseguire attraverso la forza della politica. In realtà la posta in gioco sembra più alta, poiché pertiene alla ricerca di un difficile punto di equilibrio tra la tutela dei diritti dei singoli e l'invasività delle moderne tecniche di sorveglianza elettronica, le quali non soltanto trascendono il confine tra pubblico e privato[109], ma sono insensibili alle stesse frontiere territoriali, ponendo le premesse per vere e proprie forme di *global cybersurveillance*[110]. Se questa è la natura dei conflitti sottostanti, evidentemente le risposte locali, quali quelle offerte dall'ordinamento europeo, non possono che risultare parziali e insoddi-

[108] Per alcuni rilievi in proposito v. G. Greenleaf, *International Data Privacy Agreements after the GDPR and* Schrems, in 139 *Privacy Laws & Business International Report* 12 (2016).

[109] Cfr. F. H. Cate *et al.*, *Systematic government access to private-sector data,* 2 *Int'l Data Privacy L.* 195 (2012); N. M. Richards, *The Dangers of Surveillance,* cit., 1935.

[110] Cfr. A. Arnbak – S. Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad* , cit., 319, 345-356 (ove è presentata un'articolata analisi delle tecniche utilizzate dalla NSA per intercettare o manipolare il traffico digitale anche al di fuori del territorio USA); D. Severson, *American Surveillance of Non-US Persons: Why New Privacy Protections Offer Only Cosmetic Changes,* cit.; C. Comella, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza «Safe Harbor» della Corte di giustizia dell'Unione Europea, infra* in questo Volume par. 3; più in generale A. Masferrer – C. Walker, a cura di, *Counter-Terrorism, Human Rights and the Rule of Law. Crossing Legal Boundaries in Defence of the State,* Cheltenham, 2013.

sfacenti. Si richiederebbe, invece, il rafforzamento degli strumenti offerti dal diritto internazionale, in modo da dare effettiva attuazione, adeguandoli alla realtà del contesto tecnologico, ai principi iscritti nell'art. 12 della Dichiarazione Universale dei Diritti Umani e nell'art. 17 del Patto Internazionale dei Diritti Civili e Politici[111], ove la riservatezza è elevata al rango di diritto umano, indipendentemente dalle appartenenze nazionali e territoriali. In questo senso sembrano muoversi alcuni recenti interventi dell'Assemblea Generale delle Nazioni Unite[112] e del Consiglio dei diritti umani[113], oltre alle varie dichiarazioni dei diritti che s'inscrivono all'interno del variegato universo del 'costituzionalismo digitale' contemporaneo[114]. Si tratta di segnali incoraggianti, ma la strada da percorrere è evidentemente ancora molto lunga.

[111] In proposito v. E.A. Rossi, *Il diritto alla privacy nel quadro giuridico europeo e internazionale alla luce delle recenti vicende sulla sorveglianza di massa,* in *Dir. com. sc. int.,* 2014, 331.
[112] Cfr. la Risoluzione del 18 dicembre 2013, UN Doc A/RES/68/167, *The Right to Privacy in the Digital Age*.
[113] Cfr. la Risoluzione del 1 aprile 2015, UN Doc A/HRC/RES/28/16, *The Right to Privacy in the Digital Age*, con la quale si delibera la nomina di uno *special rapporteur on privacy*.
[114] L. Gill – D. Redeker – U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights,* Berkman Center for Internet & Society, Research Pub. N. 2015-15 (9 Nov. 2015), accessibile all'indirizzo http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687120 [ultimo accesso 12.7.2016]; F. Musiani, *Une 'Charte' pour les droits des Internautes? Perspectives et alternatives,* in *Droit et société,* 2012, 425; M. Bassini – O. Pollicino, a cura di, *Verso un Internet Bill of Rigths,* Roma, 2015.

Abstract

This article focuses on the background of the ECJ Schrems decision and deals with the regulatory conflict between USA and Europe in the field of data protection. It provides a detailed analysis of the legal architecture of the mass surveillance programs adopted by the US security agencies and discusses the issue of privacy protection for foreign citizens. By comparing the US and the EU approach, it details the transatlatic conflict that arose in the aftermath of the introduction of the Directive 95/46 and looks at the ECJ Digital Rights, Google Spain and Schrems decisions as integral part of such regulatory conflict. It argues that given the particular features of the technological context, which makes extraterritorial violations much easier, decision-makers should take more seriously the universal character of the right to privacy as a fundamental human right.

Cosimo Comella

Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza Safe Harbor *della Corte di giustizia dell'Unione Europea*

Sommario: Introduzione. – 1. Sorveglianza di massa e 'adeguata protezione'. – 2. Notizie dal *Datagate* e da altri *leaks*. – 3. La crittografia e la (in)sicurezza delle comunicazioni elettroniche. – Affrettate conclusioni.

Introduzione

La recente sentenza della Corte di giustizia dell'Unione Europea nel caso *Schrems vs Data Protection Commissioner*[1], sottoposto dalla *High Court* della Repubblica d'Irlanda, lascia sullo sfondo il tema della *mass surveillance*, soprattutto nella sua articolazione tecnologica, ancorché esso emerga in più punti della decisione.

Tuttavia l'argomento che sostiene l'azione iniziale di Maximilian Schrems nei confronti di Facebook e, successivamente, del *Data Protection Commissioner* irlandese è proprio l'esistenza di programmi di sorveglianza di massa su scala globale condotti da autorità federali statunitensi, portati a conoscenza del pubblico nel corso del 2013 a seguito delle dichiarazioni di Edward Snowden e alla pubblicazione di resoconti giornalistici e documenti riservati da parte del quotidiano britannico *The Guardian* e di quello statunitense *The Washington Post*, con la diffusione di ulteriori documenti a mezzo Internet da parte dell'organizzazione *Wikileaks*: azioni informative che hanno dato vita al clamoroso caso mediatico internazionale noto come *Datagate*.

In questo articolo, dopo una generale introduzione al tema della sor-

[1] Causa C-362/14 avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte di giustizia dell'Unione Europea, ai sensi dell'articolo 267 TFUE, dalla High Court (Corte d'appello, Irlanda), con decisione del 17 luglio 2014, pervenuta in cancelleria il 25 luglio 2014, nel procedimento *Maximillian Schrems contro Data Protection Commissioner*, con l'intervento di: Digital Rights Ireland Ltd.

veglianza di massa alla luce delle informazioni sulle attività di *intelligence* diventate di pubblico dominio, ci si concentra su alcuni aspetti tecnologici della *mass surveillance* contemporanea, presentando alcune delle principali metodologie di infiltrazione di reti e sistemi informatici e di telecomunicazione per attività di SIGINT condotte nell'ambito di programmi di spionaggio o di altre attività investigative.

Viene poi fatto cenno all'utilizzo delle tecnologie crittografiche e ai loro limiti rispetto alla protezione dei dati e della riservatezza delle comunicazioni, fornendo infine alcuni dettagli su due interessanti casi che hanno suscitato particolare allarme nella comunità di sicurezza informatica internazionale e che, interpretati alla luce delle rivelazioni del *Datagate*, costituiscono un monito riguardo all'affidamento acritico o inconsapevole a strumenti tecnologici per la protezione di informazioni e comunicazioni dalla cui *disclosure* può derivare un severo pregiudizio per i diritti e le libertà di un individuo.

1. Sorveglianza di massa e 'adeguata protezione'

La sentenza della Corte di giustizia UE del 6 ottobre 2015 non affronta direttamente il tema della sorveglianza di massa, tantomeno nella sua dimensione tecnologica, quantunque sia intuibile il peso che il caso *Datagate* ha esercitato sulla valutazione dei giudici, che nella ricostruzione fornita in narrativa e nella trattazione delle questioni pregiudiziali presentate dalla *High Court* fanno emergere chiaramente riferimenti al 'diritto e la prassi in vigore' nello Stato terzo (si veda il paragrafo 66 della decisione) che «non garantiscono un livello di protezione adeguato».

È invece nel procedimento principale intentato da Schrems innanzi al *Data Protection Commissioner*, e nel successivo giudizio d'appello innanzi alla *High Court*[2], che vengono fatti più espliciti ed estesi riferimenti alle rivelazioni di Edward Snowden sulle diverse campagne di raccolta di dati svolte da agenzie governative degli Stati Uniti (con la collaborazione di analoghi organismi di altri Paesi, anche europei).

In particolare, i giudici d'appello irlandesi hanno concluso che le rivelazioni di Edward Snowden dimostrano come le autorità americane abbiano commesso «eccessi considerevoli» nelle attività condotte, ancor-

[2] Schrems -v- Data Protection Commissioner [2014] IEHC 310 (18 June 2014) – http://www.bailii.org/ie/cases/IEHC/2014/H310.html [ultimo accesso 12.7.2016].

ché volte a tutelare un interesse pubblico, aggiungendo che «la NSA e altri organi federali, come il *Federal Bureau of Investigation* (FBI), potrebbero accedere a tali dati nell'ambito della sorveglianza e delle intercettazioni indifferenziate da essi praticate su larga scala».

D'altra parte, l'esistenza di programmi di spionaggio telematico (identificati con nomi in codice e acronimi ormai divenuti di pubblica notorietà come PRISM, XKeyscore, Tempora, Bullrun e altri), oltre a non essere contestata, veniva corroborata dalla divulgazione di ordini giudiziari emessi da corti americane in base al Chapter 36 del Title 50 dello U.S. Code[3], che forniva in questo modo conferme inaspettate alle rivelazioni a mezzo stampa. Conferme che non tardarono a venire direttamente dalle stesse autorità americane, seppur riferite alle attività di spionaggio estero (*foreign intelligence*)[4].

La stessa Facebook Inc., nel rispondere alle istanze iniziali di Schrems, aveva ammesso di sottostare a «significant constraints under US law» possibile eufemismo a fronte del ricorso da parte di autorità statunitensi (anche governative e non necessariamente giudiziarie) ai c.d. *gag orders* che vincolano chi vi è sottoposto a non divulgare nulla riguardo a determinati fatti e circostanze che formino oggetto di determinati ordini dell'autorità rispetto ai quali l'interessato è parte.

Si può sostenere, quindi, che almeno a partire dal 2013 l'esistenza di attività di *mass surveillance* sulle reti di comunicazione elettronica svolte dagli Stati Uniti e da altri Paesi per finalità dichiarate di lotta al terrorismo sia una realtà incontestata, tenendo ben presente che analoghe attività sono comunque praticabili e praticate ormai in ogni parte del mondo da chi ne abbia la capacità tecnica allorquando se ne determini la possibilità e la opportunità di trarne vantaggi economici, politici, militari.

«Yet only the foolish would deny that the United States has, by virtue of its superpower status, either assumed - or, if you prefer, has had cast upon it - far-reaching global security responsibilities. It is probably the only the world power with a global reach which can effectively monitor the activities of rogue states, advanced terrorist groups and major organised crime, even if the support of allied states such as the United Kingdom is also of great assistance in the discharge of these tasks and responsibilities. The monitoring of global communications

[3] http://uscode.house.gov/browse/prelim@title50/chapter36&edition=prelim [ultimo accesso 12.7.2016]

[4] C. Savage – E. Wyatt – P. Baker, *U.S. Confirms That It Gathers Online Data Overseas*, *The New York Times,* 6 giugno 2013, http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?_r=0 [ultimo accesso 12.7.2016].

- subject, of course, to key safeguards - is accordingly regarded essential if the US is to discharge the mandate which it has thus assumed. These surveillance programmes have undoubtedly saved many lives and have helped to ensure a high level of security, both throughout the Western world and elsewhere. But there may also be a suspicion in some quarters that

this type of surveillance has had collateral objects and effects, including the preservation and re-inforcing of American global political and economic power».

(dalla decisione della High Court irlandese sul caso Schrems -v- Data Protection Commissioner - [2014] IEHC 310 – 18.06.2014)

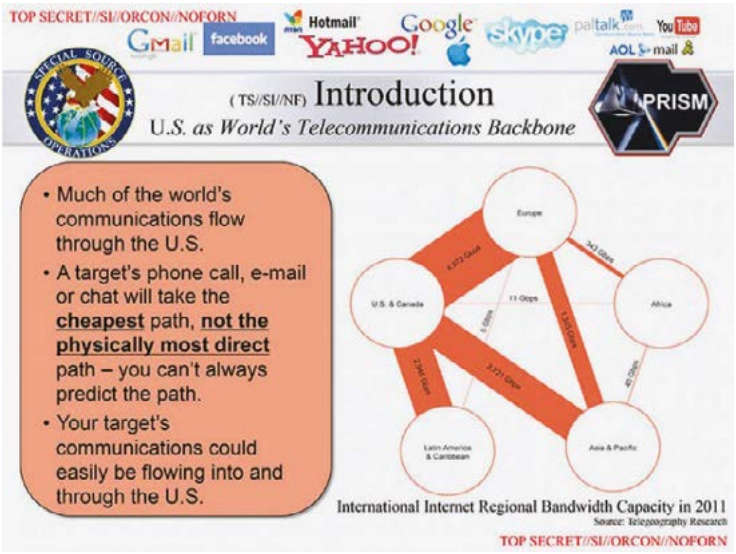
Ciò induce a qualche riflessione sullo scetticismo con cui furono accompagnate, a partire dal 1988, le notizie su un esteso *network* di SIGINT (*Signal Intelligence*) e COMINT (*Communications Intelligence*) realizzato con la cooperazione di Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda (anche allora i *five eyes* della sorveglianza globale) per l'intercettazione globale di telefonia, posta elettronica e messaggi fax: si fa riferimento a quel *sistema Echelon* che, sollevando un enorme scalpore in Europa, suscitò anche l'interesse del Parlamento Europeo, con preoccupazioni per le possibili ricadute negative su imprese e sull'economia comunitaria, oltre che sui diritti civili dei cittadini europei[5].

La capacità tecnica di agire in determinati contesti tecnologici non è ovviamente esclusiva di organismi statunitensi o dell'area occidentale: altre potenze anche di rango regionale hanno dimostrato di possedere il *know-how* e le risorse per condurre operazioni di spionaggio informatico ed elettronico di altissimo livello, oltre che di essere protagoniste del mercato della sicurezza, anche informatica, a livello mondiale. Tuttavia le autorità statunitensi hanno goduto di una condizione di oggettivo privilegio, rispetto a quelle di altri Paesi, nel condurre operazioni di *intelligence* sulla rete Internet, per evidenti circostanze di fatto: i principali operatori della società dell'informazione sono infatti di origine americana e operano prevalentemente sul territorio degli Stati Uniti, su cui si concentra una mole di informazioni e di dati personali riferibili a una parte significativa della popolazione mondiale che non ha al momento analogie in nessun altro Paese. Basti pensare, in proposito, ai *social networks* quali *Facebook* e, in misura minore, *Google+* e

[5] *The ECHELON Affair – The EP and the global interception system 1998-2002* – http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf [ultimo accesso 12.7.2016]

LinkedIn, utilizzati ogni giorno da più di un miliardo di abitanti del pianeta[6] che consegnano ai *database* di queste imprese propri dati personali rivelatori di ogni aspetto della vita privata; e, soprattutto, ai grandi fornitori di piattaforme *cloud computing*, a cominciare da Amazon che con i suoi AWS – *Amazon Web Services* – ha creato il fenomeno *cloud* globale e fornisce servizi *IaaS* (*Infrastructure as a Service*) a una parte significativa di *sub-provider* o di *service provider*. Vi sono stime per cui fino al 70% del traffico Internet mondiale attraversi, grazie alla presenza dei *datacenter* Amazon, le reti della Virginia settentrionale, negli USA, in una zona geografica storicamente ricca di insediamenti industriali ICT e di agenzie governative operanti nei settori della difesa, della sicurezza e dell'intelligence[7].

A questo proposito è di particolare interesse un'altra delle famose *slides* di Snowden che qui si riporta e che mostra graficamente i volumi di dati scambiati tra le aree geografiche del mondo, e da cui si evidenzia il ruolo degli USA quale *hub* globale delle comunicazioni elettroniche, unitamente al dato della stretta connessione tra Europa e Stati Uniti, rilevabile dai flussi di comunicazione elettronica riportati graficamente in scala in base alla capacità trasmissiva.



[6] M. Zuckerberg, *Facebook*, 27 agosto 2015 – https://www.facebook.com/zuck/posts/10102329188394581 [ultimo accesso 12.7.2016].

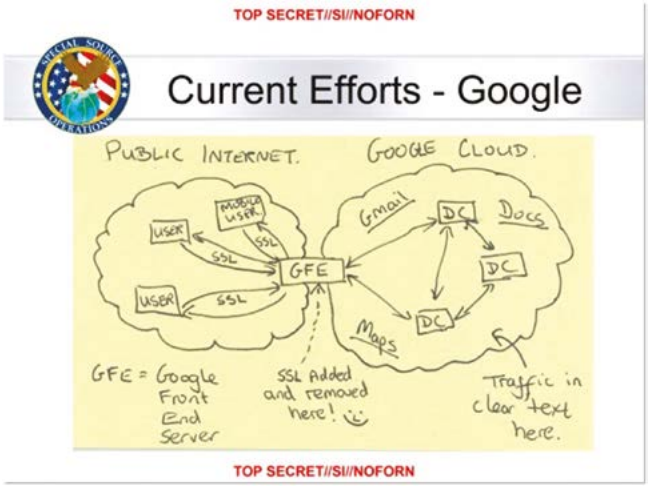
[7] *Up to 70 percent of global Internet traffic goes through Northern Virginia*, NextGov, January 8, 2016 – http://www.nextgov.com/big-data/2016/01/70-percent-global-internet-traffic-goes-through-northern-virginia/124976/ [ultimo accesso 12.7.2016]

2. Notizie dal Datagate e da altri leaks

Preso atto della realtà della *mass surveillance*, declinata in una pluralità di gradazioni che vanno dalla mera *data retention* normativamente prevista per i dati di traffico telefonico e telematico alla raccolta di informazioni frutto dell'applicazione di tecniche di *deep packet inspection* sui flussi di dati nella rete, all'acquisizione con tecniche invasive dei 'domicili digitali' praticate con l'ausilio di sofisticati sistemi *software*, è possibile analizzare, seppur sommariamente, le modalità con cui agenzie di *intelligence* e organismi investigativi possono concretamente ottenere accesso alle informazioni che quotidianamente vengono affidate al sempre più complesso e articolato ecosistema digitale.

Le tecniche di intrusione variano in base alla tipologia di comunicazione, alla selettività della ricerca che si intende svolgere, alla località geografica in cui avviene l'acquisizione del dato, alla minore o maggiore partecipazione di soggetti terzi: la casistica nota consente di individuarne alcune categorie, senza pretesa di esaustività, che qui sommariamente si discutono.

Collegamenti diretti ai datacenter delle Internet companies. Questa modalità di accesso è particolarmente rilevante nel contesto Internet, perché è quella cui risulta siano state sottoposte le maggiore aziende di comunicazione elettronica e *over the top* (OTT) che, basate negli USA, offrono servizi su scala geografica globale. In base ai documenti svelati da Snowden, le autorità statunitensi hanno potuto avere accesso diretto,



con propria connettività, alle reti interne dei maggiori operatori Internet, dei *social networks*, dei fornitori di *search engines*, dei *cloud providers* e di altri servizi di rete, considerati come veri e propri *provider* nell'ambito dei programmi PRISM, Xkeyscore, MUSCULAR.

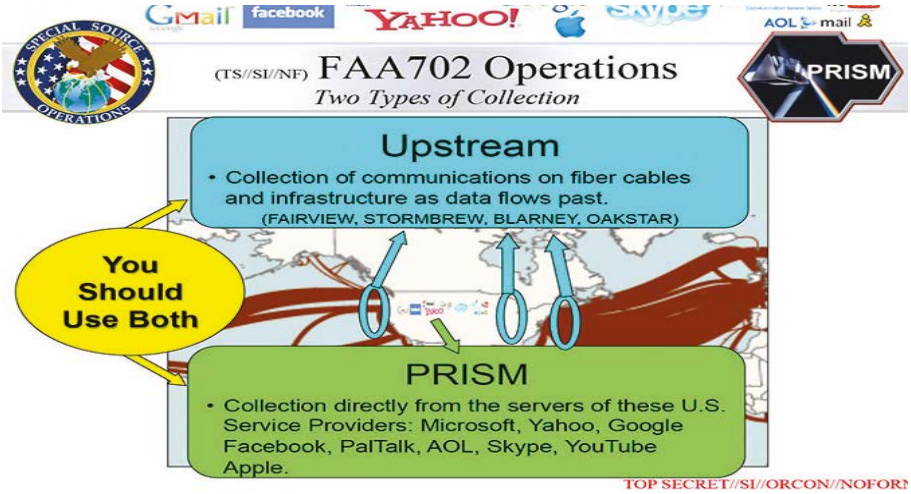
Ciò ha come immediata implicazione il fatto che la gestione da parte di un utente di propri dati tramite servizi resi, nel loro strato di presentazione, in forma di *web application* assistita da protezione crittografica (quindi con ricorso a connessioni basate su protocolli HTTPS/SSL – *Secure Socket Layer*, ingenerando nell'utente una percezione di riservatezza delle comunicazioni tra i propri dispositivi e il *service provider*) non abbia dato, e non dia attualmente, alcuna garanzia sul fatto che i medesimi dati, una volta registrati sui sistemi di *storage* nei *datacenter*, rimangano nella esclusiva sfera di conoscibilità e disponibilità dell'utente del servizio.

La protezione crittografica, infatti, pur correttamente predisposta e nei limiti della sua robustezza, è efficace solo nella fase di transito delle informazioni, mentre non è utilizzata, normalmente, quando il dato perviene alla sua destinazione presso i *server* che erogano tecnicamente il servizio, che lo elaborano per lo più 'in chiaro', per motivi di efficienza e a volte di praticabilità (essendo l'elaborazione di dati in forma crittografica ancora, in generale, argomento di ricerca e, per quel che è possibile già osservare, comunque gravata da pesanti limitazioni e penalizzazioni in *performance*).

È eloquente, a questo proposito, una delle più note *slide* fornite da Snowden, relativa allo schema delle connessioni alle reti *cloud* private di Google e Yahoo da parte degli utenti Internet, e allo 'spacchettamento' del protocollo SSL, sopra riportata.

Mentre questa modalità di accesso 'diretto', a cui fanno riferimento diversi documenti divulgati nel *Datagate*, appare tecnicamente priva di sofisticazioni, essendo basata sulla materiale accessibilità ai dati ottenuta tramite la collaborazione (spontanea o forzosa) del *service provider*, essa è quella quantitativamente più rilevante, poiché consente l'accesso indiscriminato a tutta la *customer base* delle *Internet companies* e a tutti i dati a essa collegati. In alcuni casi risultano allestiti veri e propri sistemi di interrogazione e ricerca che consentono agli analisti e agli investigatori di operare autonomamente le *query* sui *database* di interesse, siano essi costituiti dalle *spool directory* dei messaggi di posta elettronica o dai *repository* documentali dei servizi *cloud* pubblici con cui si realizzano servizi di *storage* in rete.

Nel contesto del *Datagate*, è documentata la raccolta di dati effettuata dalla NSA con questa modalità sfruttando connessioni dirette ai sistemi centrali di Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype,



YouTube, Apple[8].

Compromissione dei grandi nodi di smistamento delle comunicazioni elettroniche. In questo scenario, l'acquisizione dei dati avviene agendo sui flussi di comunicazione che attraversano le reti transcontinentali e le grandi centrali di smistamento costituite dai *router* di frontiera tra gli *autonomous systems* della rete Internet, dagli apparati di *switching* dei grandi *carrier* internazionali, dalle infrastrutture di *peering* del traffico come quelle dei c.d. *Internet eXchange Providers* (IXP) o *neutral access point* per l'interscambio 'paritario' di traffico IP, dalle reti e dagli apparati dei *transit operators*, dalle infrastrutture fisiche costitute dalle reti di cavi sottomarini in fibra ottica.

Al di là delle peculiarità di ciascuna di queste diverse infrastrutture, ciò che le accomuna è la distanza dall'utente finale, normalmente non in rapporto diretto con l'organizzazione che le gestisce, e il fungere esclusivamente da intermediatrici della comunicazione.Va da sé che reti e apparati di questa classe siano attraversati da flussi di enorme portata il cui filtraggio per la ricerca di contenuti o di dati esteriori di interesse investigativo richiede enormi capacità di elaborazione dei dati, ragionevolmente disponibili solo in strutture *ad hoc*, esterne alla rete o infrastruttura vigilata.

Il caso estremo di sfruttamento dei *landing sites* dei grandi cavi sotto-

[8] *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, *The Washington Post*, 6 giugno 2013 – https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [ultimo accesso 12.7.2016]

marini, che pure risulta tra le azioni svolte da potenze occidentali nell'ambito dei programmi di *mass surveillance* (anche in danno, parrebbe, di Paesi alleati) e che ha suscitato preoccupazione e interesse tra le autorità di protezione dati europee, è un'attività che può essere quasi esclusivamente appannaggio di apparati statali e avvenire, salvi i pur ipotizzati scenari di alto spionaggio tra potenze nemiche con le intercettazione di cavi *in the middle* sui fondali oceanici, solo grazie a forme di collaborazione da parte degli operatori responsabili delle infrastrutture o da parte di organismi di sicurezza.

Nell'ambito del *Datagate*, tale modalità di spionaggio delle comunicazioni pare sia stata adottata da organismi di sicurezza del Regno Unito, nell'ambito del programma TEMPORA condotto dal *Government Communications Headquarters* (GCHQ), ritenuto da Edward Snowden più insidioso degli analoghi programmi americani[9].

Le intercettazioni dei cavi sottomarini plausibilmente possono svolgersi attaccando le componenti elettroniche dei 'punti di rigenerazione' delle linee di comunicazione in fibra ottica, in cui i segnali vengono amplificati per compensare le attenuazioni prodotte dalla distanza. Oltretutto negli stessi punti i fasci di cavi non sono accorpati e intrecciati, e sono più facilmente manipolabili singolarmente.

Tuttavia si deve ritenere che tale tecnica rappresenti una soluzione estrema, ben potendosi raggiungere lo stesso risultato operando senza le scomodità, la complessità tecnica e i costi dell'ambiente sottomarino: i cavi oceanici hanno pur sempre un «safe harbor» a cui approdare, e sono proprio le stazioni costiere le sedi in cui più agevolmente intercettare le comunicazioni, grazie a sonde ottiche che riflettono i segnali per captare le comunicazioni senza interferirvi in modo rilevabile.

I volumi di dati in transito sui cavi transcontinentali sono enormi, e per favorirne l'analisi con il sistema TEMPORA si è predisposta una capacità tecnica di *bufferizzazione* del traffico che consente il *full dump* delle comunicazioni per 72 ore e la registrazione dei *metadati*, ovvero dei dati di traffico esteriori alla comunicazione, per 30 giorni.

Sull'onda delle polemiche seguite al *Datagate*, il Parlamento britannico ha nominato il 5 novembre 2015 (la *House of Commons*) e il 25 novembre 2015 (la *House of Lords*) una speciale *Joint Committee* per la valutazione del *Draft Investigatory Powers Bill* che regolerà, una volta approvato, le intercettazioni delle comunicazioni, la raccolta, la conservazione e l'uso

[9] *GCHQ taps fibre-optic cables for secret access to world's communications, The Guardian*, 21 giugno 2013 – http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa [ultimo accesso 12.7.2016]

dei dati, definendo le modalità della vigilanza su tali delicate attività.[10]

Tra le più significative critiche rivolte al programma TEMPORA e agli analoghi programmi di raccolta di massa di informazioni è degna di nota quella dell'ex direttore tecnico del servizio di analisi della NSA, William Binney, secondo cui le raccolte di enormi volumi di dati omnicomprensivi rischiano di avere effetti controproducenti ai fini dell'analisi, assorbendo enormi risorse per la loro interpretazione e mimetizzando nei grandi volumi di dati le informazioni di rilievo investigativo[11]. Analoga preoccupazione è stata più volte espressa, anche recentemente, dal Garante per la protezione dei dati personali in riferimento al problema generale della raccolta di dati personali a fini di sicurezza nel contesto nazionale italiano[12].

Compromissione dei nodi locali di una rete. Questa attività richiede una capacità di penetrazione su componenti minori e più capillari di una rete di comunicazioni elettroniche, ma consente, a differenza del caso precedente, una maggiore selettività dei *target* che vengono discriminati a monte, rendendo nel contempo necessaria una minore capacità di elaborazione e filtraggio, operando sugli stadi di linea e sugli apparati più prossimi al soggetto o ai soggetti di interesse investigativo. In contesti non ostili, sia dal punto di vista normativo che di fatto, o in cui non ci siano esigenze di segretezza assoluta dell'attività, l'azione è realizzata con la collaborazione dell'operatore della rete, sia esso un *carrier* telefonico, un operatore di trasmissione dati o i reparti ICT di un'organizzazione, e può comportare l'installazione di apparati *ad hoc* oppure l'utilizzo di dispositivi già in possesso dell'operatore, per acquisire dati di traffico o flussi di comunicazione. L'esfiltrazione dei dati può avvenire tramite memorizzazione su dispositivi di *storage* o tramite la disponibilità di risorse di comunicazione *out-of-the-band* che garantiscano la consegna delle informazioni digitali a un 'punto di ascolto' predisposto.

Nel caso di centrali telefoniche per telefonia fissa o mobile e in quello

[10] *Joint Committee on the Draft Investigatory Powers Bill* – http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-investigatory-powers-bill/ [ultimo accesso 12.7.2016].

[11] *GCHQ mass spying will 'cost lives in Britain,' warns ex-NSA tech chief, The Register,* 6 gennaio 2016 – http://www.theregister.co.uk/2016/01/06/gchq_mass_spying_will_cost_lives_in_britain/ [ultimo accesso 12.7.2016].

[12] *La vera minaccia è quella cibernetica, un attacco alle grandi strutture del Paese. È lì che serve più protezione.* Intervista ad Antonello Soro di Liana Milella, *La Repubblica*, 27 novembre 2015.

di nodi di smistamento di traffico Internet (con dispositivi di *routing* o di *switching* per i protocolli di rete in uso) sono di ausilio, nello scenario collaborativo, le funzionalità di *lawful interception* insite negli stessi apparati, che consentono la duplicazione della comunicazione vocale oppure, nel caso del traffico dati, il c.d. *port mirroring*.

In via teorica, le stesse funzionalità di *lawful interception* o *port mirroring* possono essere sfruttate anche in contesti non collaborativi od ostili, sfruttando una qualche capacità di accesso nascosto alla rete dell'operatore (*backdoor*), ma è ragionevole pensare che la maggior parte delle attività di acquisizione di dati e di traffico avvenga e sia avvenuta in contesti che non richiedano l'applicazione di ulteriori tecniche informatiche invasive, e ciò appare rispondere al vero soprattutto nello scenario europeo che vede la presenza di Paesi che, a diverso livello di coinvolgimento, hanno dato sostegno alle attività di *intelligence* statunitensi svelate dal *Datagate*.

Occorre osservare come le misure di sicurezza degli apparati di commutazione telefonica e degli altri sistemi che compongono una rete nazionale di telecomunicazione siano esposti a rischi di accesso abusivo al pari di ogni altro sistema informatico, ragion per cui il settore telefonico è stato destinatario, in Italia, di una serie di provvedimenti prescrittivi dell'Autorità Garante per la protezione dei dati personali che, a partire dal 2006, ha dedicato una particolare attenzione agli aspetti di sicurezza nel settore TLC nazionale, a tutela della riservatezza delle comunicazioni e dei dati a esse riferiti.

Dirottamento e attrazione del traffico. L'accesso ai flussi di comunicazione elettronica attuato tramite compromissione di canali di comunicazione o di apparati è un'attività costosa e impegnativa e, in determinati scenari, tecnicamente impraticabile o non opportuna. Ci sono infatti metodi alternativi, ben più economici e quasi altrettanto efficaci con cui ottenere il controllo di flussi di comunicazione, agendo sui protocolli di rete che governano l'instradamento dei dati sulle 'reti a pacchetto'.

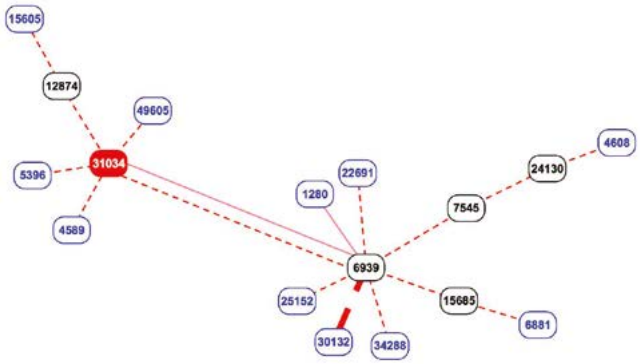
Sulla la rete Internet è noto che il protocollo utilizzato per lo scambio di informazioni sull'instradamento degli *IP datagram*, il *Border Gateway Protocol* (BGP), basa il proprio funzionamento sulla buona fede dei gestori nel trasmettere solo e soltanto *announcements* genuini, ovvero che rispecchino la reale situazione e le esigenza di instradamento delle reti appartenenti a un determinato *autonomous system* (AS).

E' stato più volte ipotizzato lo sfruttamento del meccanismo di annun-

cio e di aggiornamento delle rotte IP al fine di realizzare una sorta di 'sifonaggio' del traffico, ovvero per dirottare flussi destinati a una determinata rete verso un'altra rete o sistema autonomo senza che vi sia una seria motivazione tecnica, ma al solo fine di rendere il traffico dirottato ispezionabile o per sottrarlo al controllo del legittimo operatore[13].

Sedi preferenziali di svolgimento di questa attività sono i grandi nodi di interscambio gestiti dagli *Internet eXchange Provider* o da singole organizzazioni che gestiscono direttamente i propri router di frontiera.

Proprio la consapevolezza di queste criticità e il timore che gli IXP nazionali venissero utilizzati per realizzare operazioni di *traffic hijacking*



portarono l'Autorità Garante per la protezione dei dati personali a svolgere nel 2014 un'attività ispettiva specifica sugli IXP italiani, le cui risultanze furono condivise con le autorità nazionali di sicurezza e stimolarono, da una parte, un'azione di adeguamento tecnico da parte degli operatori interessati, dall'altra, il rafforzamento delle misure di protezione esterna da parte delle autorità di pubblica sicurezza[14].

Una inattesa conferma delle preoccupazioni dell'Autorità venne successivamente, a distanza di pochi mesi dalle attività ispettive, a seguito della

[13] *Revealed: The Internet's Biggest Security Hole, Wired.com*, August 2008 – http://www.wired.com/2008/08/revealed-the-in/ [ultimo accesso 12.7.2016].

[14] *Internet: adottate dagli Ixp le misure di sicurezza richieste dal Garante*, Newsletter n. 398 del 9 febbraio 2015 – http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3710265 [ultimo accesso 12.7.2016].

violazione dei sistemi della società milanese Hacking Team da parte di ignoti e della sottrazione in copia massiva di dati, documenti, codici programmativi e posta elettronica poi diffusi da WikiLeaks (luglio 2015)[15,16].

Si poté constatare in quella circostanza come i timori sulla corretta gestione dei flussi IP fossero stati più che giustificati: emergeva infatti come almeno una operazione di *traffic hijacking* fosse stata messa in atto nell'agosto 2013 nei confronti dell'operatore britannico Santrex, fornitore di servizi *cloud* e VPS (*Virtual Private Server*), con finalità riconducibili ad attività investigative svolte da un reparto specializzato di un corpo di polizia italiano (secondo quanto riportato, si trattava del ROS dell'Arma dei Carabinieri)[17].

A conferma delle informazioni divulgate da Wikileaks, l'analisi degli *announcements* BGP disponibile in forma storicizzata in rete tramite appositi siti, ha permesso di verificare l'accaduto nella sua evidenza tecnica e di precisarne i riferimenti temporali e i soggetti (operatori Internet) attivamente coinvolti.

Nello specifico, è risultato che il gestore dell'Autonomous System AS31034 (assegnato ad Aruba S.p.A.) a partire dalle ore 7,32 UTC del 16 agosto 2013 ha iniziato ad annunciare il prefisso IP 46.166.163.0/24. Conseguentemente, gli Autonomous Systems AS12874 (Fastweb), AS6939 (Hurricane Electric), AS49605 (Reteivo), AS4589 (Easynet) e AS5396 (MC-link) hanno iniziato ad accettare gli annunci e hanno messo in comunicazione le proprie reti, inconsapevolmente, con una rete IP appositamente configurata presso un operatore italiano per impersonare la rete dell'operatore britannico. La figura precedente, elaborata tramite BGplay, mostra schematicamente il *routing* risultante a seguito dell'annuncio surrettiziamente propagato.

L'azione di dirottamento è durata fino alle ore 13,53 UTC del 22 agosto 2013, dopodiché è stato ripristinato il normale *routing* verso la rete Sentrex. L'episodio, al di là di ogni valutazione di merito, conferma la delicatezza dell'infrastruttura Internet concepita negli anni '70 – '80 e ampiamente basata, in alcuni suoi snodi cruciali, sulla fiducia riposta nel corretto operare di alcuni soggetti che svolgono peculiari funzioni tecniche.

[15] www.wikileaks.org/hackingteam/emails/ [ultimo accesso 12.7.2016].
[16] Alex Hern, *Hacking Team hack casts spotlight on murky world of state surveillance, The Guardian*, 11 luglio 2015 – http://www.theguardian.com/technology/2015/jul/11/hacking-team-hack-state-surveillance-human-rights [ultimo accesso 12.7.2016].
[17] A. Toonk – D. Mahjoub, *How Hacking Team helped Italian Special Operations Group with BGP routing hijack* – http://www.bgpmon.net/how-hacking-team-helped-italian-special-operations-group-with-bgp-routing-hijack/ [ultimo accesso 12.7.2016].

Compromissione del terminale. Quando l'azione invasiva volta all'acquisizione di dati e informazioni si sposta dai grandi nodi delle reti verso i suoi elementi terminali, più prossimi all'utilizzatore finale, abbassandosi considerevolmente la complessità tecnologica (senza nulla togliere alla sofisticazione degli attacchi) e quindi, contestualmente, le barriere all'accesso a questo tipo di attività, lo scenario si arricchisce di nuovi attori, con la partecipazione di una più ampia platea di soggetti che producono e forniscono *software*, apparati e, soprattutto, servizi . È questo il caso delle *software house* specializzate nella produzione di strumenti intrusivi per il controllo a distanza e la 'colonizzazione' degli apparati terminali, siano essi *personal computer* o *smartphone*, in genere volti all'uso individuale. In alcuni scenari d'uso è possibile poi che il '*software* spia' venga inoculato sul terminale agendo da una sede remota rispetto all'ubicazione del *target*, mentre nella maggior parte dei casi l'inoculazione avverrà sfruttando meccanismi di *social engineering*, mediante *phishing* e *spoofing* di indirizzi di posta elettronica, oppure disponendo del materiale possesso del dispositivo da infettare. Qualora il terminale venga compromesso, comunque si giunga al risultato, verranno vanificate tutte le precauzioni eventualmente adottate, comprese quelle crittografiche, poiché lo *spyware*, agendo in modo silente e non venendo rilevato dai sistemi di protezione, avrà accesso a tutte le risorse del dispositivo, con possibilità di acquisire l'*input* da tastiera o da interfacce audio e video, e di osservare il traffico 'in chiaro' anche nel corso di sessioni assistite da protocolli di cifratura (SSL/TLS). Ciò è possibile perché, agendo sul terminale, lo *spyware* non opererà quale *man in the middle* tra le parti comunicanti, ma il suo punto di osservazione coinciderà con uno degli estremi della comunicazione in corso.

Questo genere di attacco ai sistemi terminali è sempre più diffuso per indagini giudiziarie e di polizia, e anche in Italia, pur con qualche incertezza sulla compatibilità dell'uso di tali strumenti con l'ordinamento giuridico, sembra che le possibilità di svolgimento per via tecnologica e senza la necessaria intermediazione tecnica di terzi (come i fornitori telefonici, nel caso della *lawful interception*) stia attraendo sempre più l'interesse delle forze di polizia, della magistratura inquirente e delle agenzie di sicurezza, inducendo lo sviluppo dell'offerta di servizi da parte di società specializzate che ottengono anche riconoscimenti all'estero ma godono di un significativo mercato interno fornendo supporto alle indagini giudiziarie.

3. La crittografia e la (in)sicurezza delle comunicazioni elettroniche

Del ricorso a tecniche di occultamento delle comunicazioni, soprattutto in ambito politico-militare, fornisce una straordinaria testimonianza lo storico Svetonio, nelle *Vite dei Cesari*, riferendo dello stratagemma usato da Giulio Cesare per comunicare con Marco Tullio Cicerone.

«Extant et ad Ciceronem, item ad familiares, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum, id est D pro A et perinde reliquas commutet».

Vite dei Cesari (56, I), Svetonio

Come si rileva dal testo latino, il *cifrario cesariano* consisteva in una sostituzione monoalfabetica a passo ternario (lettere A sostituita da D, B da E…) oggi di facilissima decifrazione con una elementare criptoanalisi (anche in assenza di strumenti informatici), ma molto efficace nel I secolo a.C. in cui era già un'eccezione trovare persone in grado di leggere un testo in chiaro, figurarsi quindi un testo cifrato, seppure in un modo che oggi consideriamo banale.

Le tecniche di cifratura si sono evolute dall'antichità fino al XX secolo, ma sono state accomunate dalla necessità di condivisione della conoscenza sul metodo di cifratura adottato da parte degli interlocutori, ponendo sempre il problema della scelta del canale sicuro su cui veicolare informazioni come le chiavi di cifratura condivise (cifratura simmetrica) tramite cui provvedere alla ricostruzione del testo in chiaro.

Negli anni '70 la pubblicazione dei primi risultati di ricerca su tecniche alternative 'a chiave pubblica' apriva la strada a nuovi modi di protezione delle informazioni sensibili, abilitando la comunicazione sicura su canali insicuri che è oggi alla base del funzionamento dei protocolli SSL (*Secure Socket Layer*) e TLS (*Transport Layer Security*) senza i quali non esisterebbero oggi, per esempio, il commercio elettronico o l'*home banking*.

I lavori di Rivest, Adleman e Shamir e altri[18,19], e le tecnologie che ne sono derivate, hanno aperto un'era di ottimismo riguardo alla possibilità di comunicare in modo sicuro, al riparo da orecchie e occhi indiscreti.

Oggi occorre esercitare molta attenzione perché, pur non essendo finora stati messi in discussione i principi di base della moderna crittografia a

[18] R.L. Rivest - A. Shamir – L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems,* Comm. ACM 21, 2 (Feb. 1978), 120-126.

[19] R.C. Merkle, *Secure communications over insecure channels.* Comm. ACM 21, 4 (Apr. 1978), 294-299.

chiave pubblica, esistono accorgimenti e tecniche che possono significativamente ridurre il livello di protezione o vanificarlo del tutto, esponendo le parti comunicanti allo svelamento delle proprie comunicazioni.

Si è già fatto cenno a come la contaminazione dei terminali della comunicazione eluda all'origine quasi ogni forma di protezione: la comunicazione avverrebbe in modo tecnicamente sicuro rispetto all'ascolto sul canale da parte del c.d. *man in the middle*, mentre un altro intruso potrebbe ascoltare il traffico collocandosi comodamente a uno degli estremi del cavo (in senso figurato). Un attacco di questo tipo non richiede alcuna competenza di criptoanalisi o di tecniche crittografiche, poiché l'abilità richiesta è soltanto quella necessaria a conquistare il controllo di un terminale utilizzato da una delle parti comunicanti, e una volta ottenuto questo risultato il resto verrà da sé.

Affrontiamo invece nel seguito due differenti e ben più sofisticati casi di compromissione di sistemi *software* e *hardware* in cui una più complessa linea d'azione è stata individuata, suscitando dubbi e incertezze che hanno scosso la fiducia fin qui ottimisticamente nutrita riguardo alle correnti tecniche di cifratura a chiave pubblica.

Si tratta di due casi piuttosto recenti che hanno interessato l'uno lo sviluppo degli standard crittografici adottati dall'industria informatica mondiale e l'altro un grande produttore di apparati di rete e di sicurezza, rivelando singolari e inquietanti collegamenti.

Il caso NIST/Dual_EC_DRBG

Alla base di diversi sistemi crittografici è la capacità di generare efficientemente *numeri pseudo-casuali* e *sequenze random* con più che buone qualità statistiche, da usare per comporre coppie di chiavi robuste in sistemi a chiave pubblica. Qualora le sequenze *random* generate non siano di buona qualità, e siano quindi in qualche misura prevedibili, anche a costo di un certo impegno di risorse computazionali, gli algoritmi di cifratura che le utilizzano verranno significativamente indeboliti e le informazioni con essi cifrate esposte potenzialmente ad attacchi e alla decifrazione da parte di soggetti non legittimati.

I generatori pseudocasuali utilizzati in ambito crittografico vengono chiamati *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG), e uno di questi, basato sulla c.d. crittografia ellittica (*Elliptic Curve Cryptography)*, è il Dual_EC_DRBG (*Dual Elliptic Curve Deterministic Random Bit Generator*), utilizzato a partire dal 2004 in diver-

si sistemi di cifratura.[20]

Già al momento della sua standardizzazione da parte del *National Institute of Standards and Technology* (NIST) negli Stati Uniti erano emerse nella comunità scientifica serie perplessità sull'algoritmo, perché in determinati suoi passaggi si celava la possibilità per un soggetto a conoscenza dei valori assunti da alcuni parametri matematici prefissati, utilizzati nella costruzione del generatore, di predire le sequenze *random* (che sono in effetti totalmente deterministiche, e appaiono *random* solo a un'analisi stocastica) con un limitato sforzo computazionale, potendo quindi calcolare le chiavi di decifratura per leggere in chiaro i messaggi (o analizzare in chiaro il flusso dei dati su un canale trasmissivo).

Grazie al *Datagate* seguito alle rivelazioni di Snowden si è potuto appurare, nel corso del 2013, come i dubbi sollevati da insigni matematici e criptoanalisti[21,22,23], basandosi sul dato scientificamente acquisito della potenziale vulnerabilità individuata e di cui era ignota la paternità, fossero più che fondati. Si è infatti appreso che, da una parte, la NSA aveva assicurato un cospicuo finanziamento alla società RSA perché rendesse l'algoritmo Dual_EC_DRBG come CSPRNG di *default* nei propri prodotti *software* e, nel contempo, che la stessa agenzia aveva agito affinché l'algoritmo fosse incluso nello standard ANSI X9.82 e, successivamente, in ISO/IEC 18031:2005 e in NIST SP 800-90 (dicembre 2005), assicurandone un'ampia diffusione e accettazione nell'industria informatica e negli utilizzatori.

Particolarmente interessante è il passaggio dalla standardizzazione ANSI del giugno 2004 alla pubblicazione dello standard NIST, perché nei lavori preparatori il problema della possibile vulnerabilità era stato discusso nel gruppo di lavoro, ma la formulazione artatamente adottata da NIST al momento della pubblicazione dello standard fece sì che gli implementatori fossero invogliati, rispettando la norma tecnica, ad adottare l'algoritmo Dual_EC_DRBG affinché i loro prodotti potessero conseguire la certificazione FIPS 140-2 *Security Requirements for Cryptographic Modules*

[20] *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* - NIST Special Publication 800-90A – http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf [ultimo accesso 12.7.2016].

[21] K. Gjøsteen, *Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005* – 16 Marzo 2006 – http://www.math.ntnu.no/~kristiag/drafts/dual-ec-drbg-comments.pdf [ultimo accesso 12.7.2016].

[22] *D.R. L. Brown , Conjectured Security of the ANSI-NIST Elliptic Curve RNG*, 29 Marzo 2006 – http://eprint.iacr.org/2006/117.pdf [ultimo accesso 12.7.2016]

[23] B. Schoenmakers – A. Sidorenko, *Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator*, 29 Maggio 2006 – http://eprint.iacr.org/2006/190.pdf [ultimo accesso 12.7.2016].

richiesta dalle amministrazioni USA. Questo specifico vincolo fu efficace anche tra gli sviluppatori del software *open source* OpenSSL, ampiamente usato in tutto il mondo grazie alla sua inclusione nei sistemi operativi Linux e Unix, nonostante la consapevolezza dei rischi insiti nell'algoritmo.

Dopo la pubblicazione dei retroscena dell'elaborazione dello standard NIST SP 800-90 per merito del *Datagate* il NIST ha pubblicato una sua versione aggiornata, introducendo delle misure correttive che impediscono di sfruttare la conoscenza occulta dei parametri per calcolare le chiavi di decifrazione delle comunicazioni protette.

Il caso Dual_EC_DRBG qui sinteticamente riassunto è di enorme gravità, perché dimostra come, a fronte di un interesse molto forte, agenzie dotate di particolare capacità tecnica, finanziaria e di persuasione politica possano condizionare in modo molto sottile l'evoluzione di *standard* basilari per la sicurezza delle comunicazioni in Internet, con impatto potenzialmente disastroso sulla fiducia degli utenti nella sicurezza della rete e, in caso di utilizzo distorto rispetto a quello pubblicamente dichiarato di contrasto al terrorismo, con gravissime conseguenze su diritti e libertà fondamentali degli individui, a cominciare dalla libertà di espressione.

Dal punto di vista informatico, gli studiosi di *computer science* non potranno che ricordare la frase con cui Donald E. Knuth, nel secondo volume della sua monumentale opera *The Art of Computer Programming,* ammoniva rispetto all'uso disinvolto dei generatori pseudo-casuali:

> «*Random numbers should not be generated with a method chosen at random*»[24].

L'attuale dibattito sul controllo delle reti crittograficamente protette, acuito dalle stragi di Parigi del novembre 2015, deve tenere in considerazione tutti i possibili effetti di un indebolimento programmato della sicurezza informatica delle reti, poiché gli stessi strumenti che nel mondo ritenuto libero e democratico proteggono la *privacy* delle comunicazioni e la correttezza delle transazioni finanziarie (valori considerabili possibilmente recessivi rispetto alla sicurezza e all'ordine pubblico), nei paesi non democratici o in cui non sono garantiti i fondamentali diritti umani la disponibilità di strumenti crittografici per comunicare è una delle poche forme di protezione dei cittadini e del dissenso contro lo strapotere dei regimi.

[24] D.E. Knuth, *The Art of Computer Programming – Volume 2 – Seminumerical Algorithms*, Reading, Massachusetts: Addison-Wesley, 1969.

Il caso Juniper Networks

Nel dicembre 2015 la nota azienda americana Juniper Networks, produttrice di apparati di *routing* e *switching* per reti locali e geografiche e di sistemi di sicurezza, ha segnalato tramite il proprio sito[25] l'esistenza di due vulnerabilità nei propri *firewall* dotati di sistema operativo NetScreenOS™. La notizia ha suscitato grande scalpore per via della diffusione dei sistemi Juniper e per le caratteristiche delle due differenti vulnerabilità.

Nel caso della prima vulnerabilità si trattava di una classica *backdoor* di relativamente facile scoperta: Ronald Prins di FoxIT ha per primo comunicato su Twitter di avere individuato la *password* nascosta in meno di sei ore di tempo[26] dall'annuncio di Juniper grazie a un confronto tra diverse versioni del *firmware* dell'apparato, e di averla trovata uguale alla stringa di caratteri *<<< %s(un='%s') = %u* , appositamente scelta per mimetizzarla e confonderla tra le diverse *format-string C++* presenti nel codice sorgente, nascondendola agli occhi di analisti e sviluppatori. Chi fosse stato a conoscenza della *password* avrebbe potuto accedere in modo interattivo (tramite protocolli SSH e Telnet) a uno qualsiasi dei circa 26.000 apparati NetScreen venduti da Juniper in tutto il mondo, con privilegi di amministratore di sistema, qualunque fosse la *username* utilizzata anche se non esistente nella configurazione del dispositivo.

Nel caso della seconda, ancora più grave, vulnerabilità si è trattato della possibilità di mettere in atto la temuta 'decifrazione passiva' del traffico da parte di un soggetto in grado di operare come *man-in-the-middle* sui flussi di dati trasmessi lungo circuiti VPN (*Virtual Private Network*) gestiti con apparati NetScreen.

Sono stati ipotizzati collegamenti tra la prima vulnerabilità e la seconda, nel senso che l'accesso abusivo a un sistema NetScreen consentiva la modifica di parametri crittografici delle connessioni VPN, ma è certamente la seconda vulnerabilità a destare maggiore preoccupazione e a rivestire maggiore interesse nel presente contesto.

[25] *Juniper Networks Security Incident Response – Important Announcement about ScreenOS®* - http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554 [ultimo accesso 12.7.2016].

[26] R. Prins, *Hmmm. It took @foxit 6 hours to find the password for the ssh/telnet backdoor in the vulnerable Juniper firewalls. Patch now* – https://twitter.com/cryptoron/status/677900647560253442 [ultimo accesso 12.7.2016].

Essa, infatti, si è rivelata consistere in una *backdoor crittografica*[27,28] connessa all'algoritmo Dual_EC_DRBG per la crittografia ellittica delle cui caratteristiche si è già detto, e rappresenta quindi una delle possibili applicazioni della vulnerabilità artatamente introdotta da NSA nello standard crittografico NIST SP 800-90[29].

È interessante come Juniper Networks, secondo produttore mondiale di apparati di rete dopo Cisco Systems, abbia laconicamente dichiarato, da una parte, di «non avere alcuna prova di sfruttamento della vulnerabilità su sistemi» da essa venduti, dall'altra, che «non c'è alcun mezzo per scoprire se questa vulnerabilità è stata sfruttata».

Alla luce di altre rivelazioni del Datagate, come quelle pubblicate da *Der Spiegel* nel 2013[30] e relative al software FEEDTROUGH progettato dalla NSA per creare una differente *backdoor* persistente sui sistemi firewall della Juniper, si ritiene che diversi altri produttori di apparati possano aver subito analoghe attenzioni, a cominciare da Cisco e CheckPoint, aziende *leader* di mercato della sicurezza di rete che, al pari di ogni altra azienda informatica operante nel medesimo settore, dovranno applicare ogni possibile diligenza per una revisione straordinaria dei propri codici programmativi, alla ricerca di analoghe vulnerabilità suscettibili di sfruttamento.

Affrettate conclusioni

Il caso *Snowden/Datagate* ha consentito all'opinione pubblica di toccare con mano e di misurare l'esile distanza che protegge la sfera delle comunicazioni elettroniche e dell'esperienza digitale dall'invasività della *mass surveillance* praticata per finalità di lotta al terrorismo: il difficile equilibrio tra rispetto della vita privata e tutela della sicurezza, messo a dura prova dagli scenari apertisi dopo l'11 settembre 2001 e dalle differenti sensibilità presenti nelle diverse aree del mondo rispetto alla protezione degli indi-

[27] B. Schneier, *Back Door in Juniper Firewalls*, 21 December 2015, https://www.schneier.com/blog/archives/2015/12/back_door_in_ju.html [ultimo accesso 12.7.2016].

[28] A. Langley, https://www.imperialviolet.org/2015/12/19/juniper.html [ultimo accesso 12.7.2016].

[29] CVE-2015-7755: *Juniper ScreenOS Authentication Backdoor* – https://community.rapid7.com/community/infosec/blog/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor [ultimo accesso 12.7.2016].

[30] *Shopping for Spy Gear: Catalog Advertises NSA Toolbox, Der Spiegel*, 29 dicembre 2013, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html [ultimo accesso 12.7.2016].

vidui dall'invasività e dai poteri degli Stati, costituisce oggi la sfida più importante della società dell'informazione, e richiede il coinvolgimento di competenze giuridiche, tecnologiche, di sicurezza oltre che di *intelligence*.

Nell'ambito delle azioni di monitoraggio generalizzato, le tecnologie crittografiche costituiscono un mezzo di difesa degli individui, nonché lo strumento abilitante lo sviluppo dell'economia digitale, ma sono anche armi efficaci a disposizione di organizzazioni terroristiche per comunicare eludendo l'interferenza delle legittime autorità. Al centro, il difficile ruolo di chi deve applicare le leggi, governare la complessità di fenomeni globali come il terrorismo, l'instabilità internazionale e le ondate migratorie, la criminalità organizzata, utilizzando gli strumenti che il progresso rende disponibili.

In questo senso, i recenti attacchi terroristici di Parigi e di San Bernardino negli USA hanno spinto tutte le società occidentali a interrogarsi ancora più emotivamente su cosa fare per impedire in futuro simili azioni, evocando in particolare il pericolo che il terrorismo sfrutti tecniche di cifratura delle comunicazioni, offerte anche da reti amatoriali, per operare al riparo dalle forze di polizia.

Sia in Europa che negli Stati Uniti si moltiplicano le richieste di assicurare 'entrate di emergenza' alle comunicazioni, garantendo la possibilità di accedere a informazioni e dispositivi protetti crittograficamente come i moderni *smartphone* e *tablet*.

Purtroppo la comprensibile aspirazione degli operatori e delle agenzie di *law enforcement* spesso non si traduce in una specificazione di ciò che dovrebbe essere fatto in concreto sul piano delle tecnologie, riproponendo la situazione che si creò negli USA negli anni '90 per iniziativa dell'amministrazione Clinton, sostenitrice della *key escrow* e dell'introduzione dei *Clipper Chip* sui dispositivi informatici. Ma in quell'occasione (novembre 1993) il Congresso americano ebbe la sensibilità di costituire una commissione *ad hoc* presso il *National Research Council* (NRC), ampiamente partecipata da esponenti della ricerca scientifica e della comunità di *intelligence* e di *law enforcement*, per studiare la politica nazionale riguardo alla crittografia, in quel momento vista come tecnologia abilitante il controllo delle comunicazioni e dei 'domicili digitali', per finalità di tutela della sicurezza nazionale.

Il ponderoso rapporto conclusivo[31] della commissione (di cui facevano parte, tra gli altri, Ann Caracristi, ex vice direttrice della NSA e compo-

[31] K. W. Dam – H.S. Lin, eds., Cryptography's role in securing the information society, – Committee to Study National Cryptography Policy – National Research Council NATIONAL ACADEMY PRESS, Washington, D.C. 1996.

nente del *Foreign Intelligence Advisory Board* del gabinetto Clinton, e Benjamin Civiletti, ex *U.S. Attorney General*) si tradusse in una presa d'atto della difficoltà di affrontare il problema nei termini proposti dall'amministrazione.

Infatti, relativamente alle soluzioni sul *key escrowing* la commissione osservò che qualunque regolamentazione fondata sulla disponibilità di 'chiavi di scorta' su base nazionale sarebbe stata naturalmente votata al fallimento, essendo impraticabile un accordo internazionale sui ruoli nella custodia delle chiavi e nella loro condivisione su scala planetaria, e avrebbe costituito un fattore di penalizzazione dell'industria ICT americana, poiché il mercato globale avrebbe presumibilmente rifiutato soluzioni tecnologiche caratterizzate da una capacità di controllo da parte di organismi di uno Stato estero. Inoltre, osservava come quel tipo di tecnologia si sarebbe prestato naturalmente al *dual use* a favore di regimi dittatoriali o comunque non rispettosi dei diritti umani, trasformandosi in uno strumento di ulteriore oppressione. Comunque, l'elevata complessità di un sistema articolato di *key escrow* avrebbe accresciuto il rischio di esposizione a vulnerabilità impreviste: l'esperienza dell'informatica mostra infatti come ogni sistema complesso non sia esente da difetti ed errori di programmazione (*bugs*) che sono causa di incidenti informatici che mettono a rischio la sicurezza delle banche dati nella quotidiana vita digitale.

Oggi il dibattito pubblico sulla sicurezza nella sfera digitale, condizionato dai tragici fatti di cronaca relativi al terrorismo, ci riporta a quel tempo, ma con un contesto tecnologico e sociale profondamente cambiato grazie alla pervasività della rete Internet, delle tecnologie ICT, dei *social network*, con i problemi già sul tappeto sostanzialmente irrisolti e una complessità notevolmente accresciuta, in presenza delle quali si produce una spinta verso soluzioni rapide, momentaneamente rassicuranti ma rischiose nel medio-lungo termine, che spaziano dalle già note limitazioni all'uso della crittografia alla diffusione di strumenti di controllo dei dispositivi ICT per scopi di indagine, alla raccolta massiva e duratura di dati di traffico, all'interconnessione di banche dati per finalità di sicurezza, all'analisi del traffico telematico da operare presso i grandi *Internet provider*, all'utilizzo delle funzionalità di localizzazione ormai insite in tutte le tecnologie che si interfacciano in vario modo alla rete globale.

Nell'attuale situazione sarebbe invero auspicabile una maggiore consapevolezza dei problemi e dei limiti delle tecnologie da parte di decisori politici, assemblee legislative, singoli legislatori e *opinion makers*, affinché la conciliazione delle libertà individuali e sociali con le esigenze di sicurez-

za rifugga dalle emotività e si basi esclusivamente su valutazioni razionali ponderate, rifuggendo semplificazioni e scorciatoie inefficaci che possono danneggiare e comprimere gli spazi di libertà che la nostra civiltà ha conquistato anche grazie anche ai progressi delle tecnologie dell'informazione.

Per far questo, è essenziale il coinvolgimento del mondo della ricerca scientifica e tecnologica e dell'industria ICT nazionale per consentire il necessario approfondimento dei problemi e delle possibili soluzioni; inoltre, occorre una parallela forte azione di raccordo internazionale senza la quale ogni iniziativa locale, anche da parte di Paesi tecnologicamente avanzati, rischia di sconfinare nel velleitarismo e di non produrre alcun beneficio.

Abstract

This paper addresses the mass surveillance activities revealed by Edward Snowden, emphasizing the role of the Datagate as background issue in the recent European Court of Justice decision against the EU-USA «Safe Harbor» agreement. Importance and limitations of cryptography as a self-defense weapon against the invasiveness of surveillance technologies are also briefly discussed.

The recent discovery of two different cases of vulnerability in network security equipment is described along with its relations to the Datagate, whilst readers are cautioned against placing blind confidence in cryptographic technology to protect sensitive data.

Oreste Pollicino - Marco Bassini

La Carta dei diritti fondamentali dell'Unione europea nel reasoning *dei giudici di Lussemburgo*

1. Da Digital Rights Ireland *a* Schrems*: l'epopea di un nuovo diritto alla privacy?*

Per il costituzionalista appassionato di teoria ss dell'argomentazione[1] l'analisi della sentenza *Schrems*[2] presenta una particolare rilevanza (anche) per una fortunata coincidenza cronologica[3]: la decisione della

[1*] Il presente contributo costituisce l'esito di uno sforzo congiunto dei due Autori. Nondimeno, sono da attribuirsi a Oreste Pollicino i paragrafi 2, 5, 6 e 7 e a Marco Bassini i paragrafi 1, 3 e 4. Più in generale, sui temi dell'argomentazione giuridica delle corti in campo 'digitale', si v. P. Costanzo, *Il fattore tecnologico e le sue conseguenze,* in *Rass. Parl.,* 2012, 4, 811. Sia consentito rinviare anche a O. Pollicino, *La «transizione» dagli atomi ai bit nel* reasoning *delle Corti europee,* in *Ragion pratica,* 2015, 1, 53.

[2] Corte di giustizia UE, 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner.*

[3] Per i primissimi commenti 'a caldo', si v. S. Rodotà, *Internet e privacy, c'è un giudice in Europa che frena gli Usa,* in www.repubblica.it, 12 ottobre 2015; M. Scheinin, *The Essence of Privacy, and Varying Degrees of Intrusion,* in www.verfassungsblog.de, 7 ottobre 2015; R. Miller, *Schrems v. Commissioner: A Biblical Parable of Judicial Power*, *ivi,* 7 ottobre 2015; C. Kuner, *The Sinking of Safe Harbor, ivi*, 8 ottobre 2015; O. Lynskey, *Negotiating the Data Protection Thicket: Life in the Aftermath of Schrems, ivi,* 9 ottobre 2015; S. Peers, *The party's over: EU data protection law after the Schrems Safe Harbor judgment,* in www.eulawanalysis.blogspot.it, 7 ottobre 2015; M. Nino, *La Corte di giustizia UE dichiara l'invalidità del sistema di Safe Harbor: la sentenza Schrems,* in www.

Commissione che aveva omologato i principi del *Safe Harbor,* su cui si appunta la pronuncia della Corte di giustizia, risale al 26 luglio 2000[4], pochi mesi prima della proclamazione (7 dicembre 2000) della Carta di Nizza.

La questione sembra potersi porre, così, in questi termini: la proclamazione, prima, e l'entrata in vigore, dopo (solo a partire dal dicembre del 2009), della Carta e in particolare, il portato degli artt. 7 e 8 (e 47) della stessa hanno, di fatto, determinato la caducazione di un atto *originariamente* compatibile con il diritto dell'Unione europea, a causa di una sua 'rilettura' alla luce del nuovo parametro?

Tale interrogativo, come appena accennato, presenta motivi di interesse peculiari alla luce della tendenziale coincidenza tra il periodo in cui la Carta ha visto la luce, seppure in via di *soft law*, e quello in cui la decisione è stata adottata dalla Commissione.

Dunque, ciò che si cercherà di cogliere è se, volendo semplificare, l'avvento della Carta abbia prodotto un'ondata 'costituzionalizzatrice', ossia una reazione, da parte della Corte di Lussemburgo, consistita nello scrutinio degli atti già in vigore diretto a verificarne la coerenza rispetto ai valori proclamati nella Carta stessa .

Un'indagine in questa direzione potrebbe avvalersi del precedente costituito dalla sentenza *Digital Rights Ireland*[5], che annullando la direttiva 2006/24/CE[6] sull'assunto della incompatibilità delle disposizioni in

---

sidis-isil.org, 24 ottobre 2015; F. Coudert , *Schrems vs. Data Protection Commissioner: A Slap on the Wrist for the Commission and New Powers for Data Protection Authorities,* in www.europeanlawblog.eu, 15 ottobre 2015; P. Falletta, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C-362/14),* in www.federalismi.it, 23 dicembre 2015; A. Pulighеddu, *Il caso Schrems-Facebook: analisi e profili di collegamento con la sentenza Google Spain,* in www.dimt.it, 2 dicembre 2015. Sia consentito rinviare anche a M. Bassini - O. Pollicino, *La Corte di giustizia demolisce il* safe harbor *e ridisegna i confini del diritto alla privacy in ambito transnazionale*, in www.diritto24.ilsole24ore.com, 7 ottobre 2015..

[4] Decisione 2000/250/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti.

[5] Corte di giustizia UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland, Seitlinger e a.*

[6] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

tema di conservazione dei dati di traffico con gli artt. 7 e 8 della Carta, ha di fatto offerto una rivisitazione 'costituzionalmente' orientata di quella disciplina.

Anche in un particolare passaggio della pronuncia in esame, tuttavia, e precisamente al punto 72, sembra cogliersi nuovamente quell'attitudine a un'interpretazione espansiva, quasi manipolativa, delle disposizioni contenute nella direttiva, secondo una deviazione, non si fatica a credere volontaria, incline a garantire alla tutela dei dati personali il più ampio spazio: la Corte attribuisce all'art. 25, par. 6, della direttiva 95/46/CE[7], la norma su cui poggia il potere della Commissione di constatare l'adeguatezza del livello di protezione dei dati personali offerto da un paese terzo, lo scopo di assicurare la *continuità* (quasi un prolungamento spaziale della tutela giuridica) del grado elevato di protezione che la direttiva mira a stabilire all'interno dell'Unione europea.

È uno tra i più significativi dei passaggi in cui emerge questa attitudine a una lettura espansiva, che si era già manifestata e osservata nelle altre pronunce che hanno ormai contribuito a definire lo statuto giurisprudenziale della privacy digitale[8]. Anche nei casi *Digital Rights Ireland* e *Google Spain*[9], infatti, la Corte di giustizia era parsa muoversi nell'orizzonte di ampliare il più possibile il margine di protezione dei dati personali e della privacy degli individui[10]. Ebbene, nella fattispecie, sembra che la Corte di

[7] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[8] Si v. sul punto il contributo su qusto Volume di G. Finocchiaro, *La giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems, p. 779.* Sia consentito rinviare, in proposito, a O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di Google Spain,* in G. Resta-V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* Roma, 2015, 7 ss.; Id., *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale,* in www.federalismi.it, 24 novembre 2014; Id., *Diritto all'oblio e conservazione di dati. La Corte di giustizia a piedi uniti: verso un* digital right to privacy, in *Giur. Cost.,* 2014, 3, 2949 ss.; O. Lynskey, *Deconstructing data protection: the 'added value' of a right to data protection in the EU legal order,* in 63(3) *International and Comparative Law Quarterly* (2014), 569.

[9] Corte di giustizia UE, 13 maggio 2014, C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja Gonzàlez.*

[10] Per alcuni commenti, cfr., riguardo alla pronuncia *Digital Rights Ireland*: L. Trucco, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali,* in *Giur. it.,* 2014, 8-9, 1850 ss.; R. Flor, *La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. «data retention» contraria ai diritti fondamentali. Una lunga storia a lieto fine?,* in *Riv. Trim. di Diritto penale contemporaneo,* 2014, 2, 178 ss.; Id., *Dalla 'Data retention' al diritto all'oblio, dalle paure orwelliane alla recente giurisprudenza*

giustizia non si sia astenuta ma abbia anzi dato seguito a questa attitudine: a costo di abbracciare, a tratti, un approccio formalistico che ha prevalso in ragione della protezione 'sostanziale' da assicurare al diritto alla protezione dei dati personali. È ciò nonostante il taglio piuttosto pragmatico adottato dai giudici nell'esame delle peculiarità dell'ordinamento statunitense.

In questo modo, l'argomentazione della Corte sembra dare a tratti credito alle opinioni di molti dei commentatori che hanno indicato nella sentenza *Schrems* la reazione, in parte anche emotiva, dell'Europa allo scandalo NSA e alle operazioni di sorveglianza globale messe in atto dal governo degli Stati Uniti, dietro il consenso o quantomeno la complicità (forse inconsapevole) di alcuni Stati membri[11]: un contesto nel quale, stan-

della corte di giustizia, in G. Resta-V. Zeno-Zencovich (a cura di), *op. cit.,* 223 ss.; A. Vedaschi-V. Lubello, *Data retention and its implications for the fundamental right to privacy*: *a European perspective,* in 20(1) *Tilburg Law Review* (2014), 14; M. Nino, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Il Dir. dell'Unione europea,* 2014, 4, 803 ss.; F. Fabbrini, *The European Court of Justice Ruling in the Data Rentention Case and its Lessons for Privacy and Surveillance in the U.S.*, 28 *Harvard Human Rights Journal* (2015), 65; E. Colombo, *Data retention e Corte di Giustizia: riflessioni a prima lettura sulla declaratoria di invalidità della Direttiva 2006/24/CE*, in *Cass. pen*., 2014, 7-8, 2705 ss. Con riferimento alla pronuncia *Google Spain,* invece, si segnalano, *ex multis,* oltre al già ricordato Volume di G. Resta-V. Zeno-Zencovich (a cura di), *op. cit.,* che reca i contributi di T.E. Frosini, O. Pollicino, G. Finocchiaro, P. Piroddi, G. Sartor-M. Viola De Azevedo Cunhia, A. Mantelero, S. Sica-V. D'Antonio, C. Comella, G.M. Riccio, R. Flor e F. Pizzetti, già apparsi sul numero speciale di *Dir. Inf.* 2014, 4-5: T.E. Frosini, *Diritto all'oblio e Internet,* in www.federalismi.it, 10 giugno 2014*;* F. Pizzetti, *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni, ivi,* 10 giugno 2014; G.E. Vigevani, *Identità, oblio, informazione e memoria in viaggio da Strasburgo a Lussemburgo, passando per Milano,* in *Danno e resp.,* 2014, 7, 731 ss.; C. Blengino, *La Corte di giustizia e i motori di ricerca: una sentenza sbagliata,* in www.medialaws.eu, 19 maggio 2014; G. Corrias Lucente, *Ancora su Google e il diritto all'oblio, ivi,* 24 giugno 2014. Sia consentito altresì rinviare a O. Pollicino-M. Bassini, *Reconciling Right to Be Forgotten and Freedom of Information: Past and Future of Persona Data Protection in Europe,* in *DPCE,* 2014, 2, 641; M. Bassini, *Il diritto all'oblio ai tempi di Internet: la Corte di giustizia sui motori di ricerca,* in *Quad. cost.,* 2014, 3, 730.

[11] Per alcune reazioni istituzionali invece, cfr. European Commission, *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems),* Bruxelles, 6 novembre 2015; Id., *Statement, First Vice-President Timmermans and Commissioner Jourová's press conference on Safe Harbor following the Court ruling in case C-362/14 (Schrems),* 6 ottobre 2015; Article 29 Working Party, *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems*

do a un piano giuridico, gli Stati Uniti non garantirebbero i presupposti per una tutela efficace, esponendo a pregiudizio i dati personali trasferiti dall'Unione europea soprattutto nell'ambito dei trattamenti effettuati da autorità pubbliche.

Il risvolto sotto il versante argomentativo di questa operazione manipolativa sembra coincidere con una trasformazione del principio di adeguatezza, cui la direttiva 95/46/CE, all'art. 25, àncora la valutazione della legittimità del trasferimento di dati personali verso paesi terzi, in principio di protezione sostanzialmente equivalente della tutela dei diritti fondamentali in gioco[12].

Tale trasfigurazione del contenuto del test alla base della legittimità dei trasferimenti di dati personali verso paesi terzi, abbastanza evidente in diversi passaggi della sentenza, di cui si dirà, si giustifica con l'intento di offrire una rinnovata e rinvigorita interpretazione dei diritti fondamentali alla privacy e alla tutela dei dati personali. La lettera della direttiva, testo ormai consolidato da più vent'anni , quando lo sviluppo di Internet era di fatto agli albori e le sue implicazioni critiche per la tutela della privacy erano ancora in larga parte sconosciute, ha così formato oggetto di un processo di (neanche troppo velata) manipolazione che, dietro un'evidente pressione per un rafforzamento delle tutele nel rapporto con l'ordinamento statunitense, ha condotto all'annullamento della decisione con cui la Commissione si era espressa in punto di adeguatezza. Con una motivazione, tuttavia, che rispecchia indirettamente l'insufficienza di questo criterio, in surrogazione (interpretativa) del quale viene utilizzato il parametro relativo alla equivalenza sostanziale della protezione.

Diversamente, non si comprenderebbe il motivo per cui, all'atto dell'adozione della decisione[13], quando la Carta dei diritti fondamentali ora

v Data Protection Commissioner case (C-362-14), WP 230, Bruxelles, 16 ottobre 2015; Federal Trade Commission, *Transatlantic Privacy After Schrems: Time for An Honest Conversation,* relazione del Commisioner Julie Brill, Amsterdam Privacy Conference, 23 ottobre 2015.

[12] IIn sintesi, l'art. 25 della direttiva 95/46/CE stabilisce che il trasferimento di dati personali verso paesi terzi può aver luogo soltanto se il paese di destinazione garantisca un livello di protezione adeguato, fatte salve le misure nazionali di attuazione della altre disposizioni della direttiva. Il compito di valutare l'adeguatezza del livello di protezione offerto da un paese terzo è affidato alla Commissione dal par. 6 dell'art. 25, secondo la procedura regolata all'art. 31 della direttiva. Nel caso la Commissione constati l'inadeguatezza del livello di tutela assicurato da un paese terzo, gli Stati membri sono tenuti ad adottare le misure necessarie a evitare ogni trasferimento di dati personali verso tale stato.

[13] Invero, come ricorda S. Rodotà, *op. cit.,* l'adozione della decisione di constatazione

così valorizzata stava per vedere la nascita, ma il suo spirito non avrebbe potuto non influenzare le scelte del legislatore europeo, seppure a titolo di *moral suasion*, la Commissione abbia potuto licenziare un atto con il quale si accertava la sostanziale adeguatezza delle garanzie previste dall'ordinamento statunitense in materia di trattamento dei dati personali[14]. A maggior ragione, questa considerazione deve valere a comparto normativo invariato, stante l'assenza di modifiche che abbiano investito le disposizioni dell'ordinamento statunitense in materia.

Così, le valutazioni condotte dalla Corte di giustizia, se investono direttamente la decisione adottata dalla Commissione, concernono in larga parte le garanzie (non) previste dall'ordinamento statunitense, risolvendosi in un apprezzamento della loro equivalenza (sostanziale) rispetto al quadro dettato dalla direttiva 95/46/CE in Europa. Il sistema del *Safe Harbor* e i principi che vi sono racchiusi costituiscono pertanto il parame-

dell'adeguatezza del sistema di *Safe Harbor* statunitense da parte della Commissione era stata accompagnata da alcune riserve espresse specialmente dal Working Party Article 29, ai tempi presieduto proprio dal Prof. Rodotà. Non è mistero che la decisione costituisca il frutto di un lungo *iter* di discussione e negoziato che ha attraversato fasi alterne, e che tradisce l'ambiguità del giudizio che si trova racchiuso nella constatazione operata dalla Commissione. Per alcuni riferimenti, cfr. Article 29 Working Party, *Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government,* 26 gennaio 1999, 5092/98/EN/final, WP 15; Id., *Opinion 2/99 on the Adequacy of the «International Safe Harbour Principles» issued by the US Department of Commerce on 19th April 1999,* 3 maggio 1999, 5047/99/EN/final, WP 19; Id., *Opinion 4/99 on The Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed «Safe Harbour Principles»,* 7 giugno 1999, 5066/99/EN/final, WP 21; Id., *Working document on the current state of play of the ongoing discussions between the european Commission and the United States Government concerning the «International Safe Harbour Principles»,* 7 luglio 1999, 5079/99/EN/final, WP 23; Id., *Opinion 7/99 On the Level of Data Protection provided by the «Safe Harbor» Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce,* 3 dicembre 1999, 5146/99/EN/final, WP 27*;* Id., *Opinion 3/2000 on the EU/US dialogue concerning the «Safe Harbor» arrangement,* 16 marzo 2000, 5019/00/EN/final; Id., *Opinion 4/2000 on the level of protection provided by the «Safe Harbour Principles»,* 16 maggio 2000, CA07/434/00/EN, WP 32. Si v. anche, più in generale, Article 29 Working Party, *Discussion Document: First orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy,* 26 giugno 1997, XV D/5020/97-EN final, WP 4; Id., *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive,* 24 luglio 1998, DG XV D/5025/98, WP 12.

[14] Per un'analisi dettagliata del sistema di *Safe Harbor,* v. in questo numero il contributo di S. Sica – V. D'Antonio, *I Safe Harbor Privacy Principles: genesi, contenuti, criticità,* p. 801.

tro interposto al quale i giudici di Lussemburgo si riferiscono per valutare la legittimità della decisione della Commissione.

Inutile negare che il portato degli artt. 7 e 8 della Carta, formalmente non coinvolti in questa 'triangolazione' tra decisione, direttiva e *Safe Harbor*, sia in realtà decisivo. È proprio la valorizzazione delle disposizioni della Carta, infatti, che permette alla Corte di giustizia di elevare, da un lato, la valutazione generale sul livello di protezione offerto dalla direttiva, e dall'altro, lo standard di 'tolleranza' per legittimare il trasferimento di dati personali fuori dall'Unione europea, convertendo –come detto- in equivalenza il parametro, formalmente incardinato nell'art. 25 della direttiva, di adeguatezza.

Mutato così il paradigma cui informare la valutazione da parte della Corte di giustizia, è stato per quest'ultima gioco facile addivenire all'annullamento della decisione.

Si potrebbe inoltre porre in questione se abbia rivestito maggiormente carattere politico la decisione che è stata oggetto di annullamento ovvero la sentenza che l'ha decretata, vale a dire se i motivi che hanno condotto la Commissione, nel 2000, ad affermare forse anche per ragioni non meramente giuridiche l'adeguatezza del sistema di *Safe Harbor* siano prevalenti rispetto a quelli che hanno guidato la Corte di giustizia verso un'opposta, seppure 'manipolata' (nei termini che si chiariranno) valutazione.

2. Gli indizi di una (nuova) manipolazione

Dove emerge maggiormente questa tendenza alla manipolazione favorita dagli artt. 7[15], 8[16] e 47[17] della Carta?

La Corte ne fa quasi una dichiarazione di intenti quando, con una impostazione ricorrente ma tutt'altro che retorica, esordisce nel suo ragionamento con l'affermazione per cui «le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al rispetto della vita

[15] Per un'analisi, cfr. T. Groppi, *Rispetto della vita privata e della vita familiare,* in R. Bifulco-M. Cartabia-A. Celotto (a cura di), *L'Europa dei diritti. Commento alla Carta dei diritti fondamentali dell'Unione Europea,* Bologna, 2001, 76 ss.

[16] Si v. F. Donati, *Protezione dei dati di carattere personale,* in R. Bifulco-M. Cartabia-A. Celotto (a cura di), *op. cit.,* 83 ss.

[17] Al riguardo, si v. M. D'Amico, *Diritto a un ricorso effettivo e a un giudice imparziale,* in R. Bifulco-M. Cartabia-A. Celotto (a cura di), *op. cit.,* 319 ss.

privata, devono essere necessariamente interpretate alla luce dei diritti fondamentali garantiti dalla Carta»[18].

Si tratta di una premessa metodologica e argomentativa che si presta senz'altro a diverse interpretazioni ma che, alla luce del risultato conseguito dalla Corte, sembra preparare il terreno per un'operazione che non si é limitata a una stretta interpretazione del dettato normativo.

È come se i giudici di Lussemburgo intendessero rivestire di una portata 'costituzionalizzante' e «fundamental rights oriented» una cornice normativa, quella definita appunto dalla direttiva 95/46/CE, che ancora ne era estranea, risalendo a un'epoca in cui la tutela dei diritti fondamentali ancora non era avvertita come pertinente all'Unione europea, alle sue istituzioni e, soprattutto, al suo diritto[19]. Nel formulare questo passaggio, la Corte sembra immaginare un rapporto *a contrario* (il che, effettivamente, da un punto di vista storico è) tra norme di diritto primario e norme di diritto derivato: secondo i giudici, poiché la direttiva investe un ambito che può «arrecare pregiudizio» alle libertà fondamentali, occorre ricorrere a un'interpretazione illuminata dalle garanzie stabilite dalla Carta[20]. Ci si

[18] Così al punto 38.

[19] Per apprezzare il cammino dell'Unione europea e dell'integrazione comunitaria, può essere utile rinviare a P. Bilancia, *The Dynamics of the EU Integration and the Impact on the National Constitutional Law. The European Union After the Lisbon Treaties,* Milano, 2012

[20] Sul contributo della Carta dei diritti fondamentali dell'Unione europea, cfr. *ex multis,* oltre a R. Bifulco-M. Cartabia-A. Celotto (a cura di), *op. cit.,* anche A. Manzella-P. Melograni- E.O. Paciotti- S. Rodotà (a cura di), *Riscrivere i diritti in Europa. Introduzione alla Carta dei diritti fondamentali dell'Unione europea,* Bologna, 2001; G.F. Ferrari (a cura di), *I diritti fondamentali dopo la Carta di Nizza. Il costituzionalismo dei diritti*, Milano, 2001; A. Barbera, *La Carta dei diritti:una fonte di ri-cognizione?*, in *Il Dir. dell'Unione europea*, 2001, 2-3, 241; R. Toniatti, *Diritto, diritti, giurisdizione. La carta dei diritti fondamentali dell'Unione europea,* Padova, 2002; A. Pace, *A che serve la Carta dei diritti fondamentali dell'Unione europea? Appunti preliminari,* in *Giur. Cost.,* 2001, 1, 193 ss.; G. Zagrebelsky (a cura di), *Diritti e Costituzione nell'Unione Europea,* Roma-Bari, 2003; A. Ruggeri, *La 'forza' della Carta europea dei diritti,* in *DPCE,* 2001, 1, 182 ss.; A. von Bogdandy, *Comunità di diritti fondamentali come meta dell'integrazione? I diritti fondamentali e la natura dell'Unione europea,* in *Dir. pubbl.,* 2001, 1, 849 ss.; L.S. Rossi (a cura di), *Carta dei diritti fondamentali e costituzione dell'Unione europea,* Milano, 2002; S. Mangiameli, *La Carta dei diritti fondamentali dell'Unione europea*, in *DPCE*, 2001, 1, 173 ss. Più recenti E. Gianfrancesco, *Some considerations on the juridical value of the Charter of Fundamental Rights before and after the Lisbon Treaty,* in www.forumcostituzionale.it, 14 febbraio 2008; S. Gambino, *I diritti fondamentali dell'Unione europea fra trattati (di Lisbona) e Costituzione,* in www.federalismi.it, 13 gennaio 2010; L. Trucco, *Tecniche di normazione e tutela dei diritti fondamentali nella Carta dei diritti fondamentali dell'Unione europea,* in A. Ruggeri-L. D'Andrea-A. Saitta-G. Sorrenti

aspetterebbe, forse, un'inversione logica: la direttiva declina su un terreno che è crocevia di diversi diritti fondamentali le disposizioni della Carta[21], istituendo un *framework* che ne assicuri la protezione secondo una massima estensione.

Subito dopo[22], però, la Corte riconosce che già la direttiva porta con sé i germi per una tutela dei diritti fondamentali in questione, così smentendo l'idea di una direttiva 'indifferente' al portato sostanziale che sarà affermato anche dalla Carta, evocando quelle disposizioni e quei considerando che annunciano come la direttiva non intenda soltanto tutelare in modo completo ed efficace quei diritti, ma più specificamente miri ad assicurarne un elevato livello di protezione.

Il secondo passaggio in cui sembra cogliersi evidenza dell'attitudine amplificatrice che caratterizza la pronuncia della Corte di giustizia si colloca nella valutazione che i giudici compiono rispetto all'estensione dei poteri delle autorità di protezione dei dati personali.

Il tema oggetto dei quesiti in via pregiudiziale, segnatamente, concerneva la possibilità di sindacare, da parte di un'autorità nazionale, l'adeguatezza delle tutele offerte da paesi terzi nei quali i dati personali erano trasferiti. In particolare, la Corte era stata richiesta di stabilire se a fronte di una decisone come quella adottata dalla Commissione e oggetto di annullamento, le autorità conservassero un margine di sindacato o fossero vincolate dall'apprezzamento condotto in quella sede dalla Commissione stessa.

Nel pervenire a una statuizione che depone in favore della possibilità di sindacare il contenuto della decisione, la Corte di giustizia non manca, nel suo percorso argomentativo, di soffermarsi in maniera diffusa sui poteri di cui le autorità dispongono, enfatizzandone il ruolo anche ai sensi dell'art. 8, par. 3, della Carta. Non si può non cogliere una lettura ampia e a tratti enfatica del ruolo delle autorità, che collega all'effettività dell'esercizio dei rispettivi poteri istituzionali la facoltà di contrastare le valutazioni della Commissione.

(a cura di), *Tecniche di normazione e tutela dei diritti fondamentali*, Torino, 2007, 317 ss.; G. Vettori, *La lunga marcia della Carta dei diritti fondamentali dell'Unione europea*, in *Riv. dir. priv*., 2007, 4, 5 ss.; A. Pizzorusso, *Il patrimonio costituzionale europeo,* Bologna, 2002.

[21] Per approfondire, si vv. anche i commenti di J. Vedsted-Hansen, *Commentary on Article 7* e di H. Kranenborg, *Commentary on Article 8,* entrambi in S. Peers-T. Hervey-J. Kenner-A. Ward (eds.), *The EU Charter of Fundamental Rights – A Commentary,* Oxford, 2014, rispettivamente 153 ss. e 223 ss.

[22] Si v. il punto 39.

Nel qualificare tale potere, lo stesso argomento utilizzato dalla Corte di giustizia si segnala per l'attenzione alla dimensione individuale di tutela dei diritti. Preliminarmente, la sentenza ricorda che una decisione della Commissione, fintantoché non sia dichiarata invalida dalla Corte di giustizia, organo a ciò competente, spiega effetti vincolanti nei confronti degli Stati membri e dei rispettivi organi[23]. Ad avviso della Corte, però, l'esistenza di una simile decisione non può precludere le necessarie vie di ricorso per gli individui i cui dati sono trasferiti verso paesi terzi presso le competenti autorità di regolazione, come previsto dall'art. 28, par. 4, della direttiva. E qui viene in rilievo soprattutto l'art. 47 della Carta (norma che si occupa del diritto 'tramite': al giusto processo), prima ancora che le norme sul contenuto della tutela (privacy e dati personali). Per altro verso, osserva la Corte[24], nemmeno una decisione siffatta può ridurre i poteri conferiti alle autorità di regolazione nell'apprestare tutela ai diritti degli interessati.

Qui la manipolazione passa per il tramite di un parametro verrebbe da dire, impropriamente, 'interposto': ossia attraverso lo scudo rappresentato dai poteri facenti capo alle autorità nazionali di regolazione nel conoscere eventuali domande da parte degli interessati. Secondo la Corte di giustizia, l'adozione di una decisione da parte della Commissione che accerti l'adeguatezza delle tutele previste dall'ordinamento statunitense non esclude dall'ambito di competenza delle autorità nazionali[25] il controllo sul trasferimento di dati verso paesi terzi né crea alcuna eccezione al riguardo[26].

E qui si giunge alla terza apparente forzatura interpretativa: laddove la Corte rileva che «sarebbe contrario al sistema predisposto dalla direttiva 95/46 […] se una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, di detta direttiva avesse come effetto di impedire a[d] un'autorità nazionale di controllo di esaminare la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al

[23] Cfr. il punto 51.

[24] Osserva la Corte al punto 52: «fintantoché la decisione della Commissione non sia stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi, fra i quali figurano le loro autorità di controllo indipendenti, non possono certo adottare misure contrarie a tale decisione, come atti intesi a constatare con effetto vincolante che il paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato. Infatti, gli atti delle istituzioni dell'Unione si presumono, in linea di principio, legittimi e producono pertanto effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità».

[25] Punto 54.

[26] Punto 55.

trattamento dei suoi dati personali che sono stati o potrebbero essere trasferiti da uno Stato membro verso un paese interessato da tale decisione»[27].

Questo ragionamento, che la Corte segue al fine di rendere esplicita l'amplificazione della tutela della privacy e dei dati personali, sembra sortire un esito paradossale, che ben si comprende dando prosecuzione alla lettura della pronuncia. Se, da un lato, la Corte di giustizia ammette che l'adozione di una decisione sull'adeguatezza del *Safe Harbor* non presenta la capacità di paralizzare le tutele azionabili avanti alle autorità nazionali di regolazione, per altro verso i giudici del Lussemburgo, nel ricordare la natura vincolante di tale decisione per gli Stati membri e i rispettivi organi, sembrano incorrere in una contraddizione logica finendo con il negare, di fatto, quel monopolio interpretativo che la Corte si era auto-attribuita nel segnare il limite all'efficacia di una decisione.

Si apre così una breccia importante che, seppure passi direttamente per il canale dell'art. 47 della Carta, relativo al diritto a un ricorso effettivo e a un giudice imparziale, conduce indirettamente a un rafforzamento sostanziale delle garanzie previste dagli artt. 7 e 8, e in particolare, come si sottolinea al punto 58, dall'art. 8, par. 3. Riaffermando la facoltà per le autorità nazionali di conoscere eventuali ricorsi degli interessati, si apre una seconda via per mettere in discussione quel giudizio di adeguatezza incorporato nella decisione della Commissione oggetto di annullamento.

Per sfuggire alla contraddizione logica (almeno apparente) ora denunziata, i giudici si premurano subito di precisare che il sindacato sulla validità degli atti adottati dalle istituzioni dell'Unione europea appartiene in via esclusiva alla Corte. Prospettando così un'alternativa secca, nell'ipotesi di ricorso avanti alle autorità nazionali: nel caso la domanda sia respinta, l'interessato potrà impugnare tale pronuncia in sede giurisdizionale, dove il giudice avrà facoltà, qualora dubiti dell'adeguatezza delle tutele offerte dal paese terzo, di investire la Corte di giustizia di una questione pregiudiziale di validità della decisione[28]; nel caso di accoglimento della domanda, invece, sarà la stessa autorità di regolazione a poter adire gli organi giurisdizionali, segnalando le criticità in ordine alla conformità della decisione all'ordinamento 'costituzionale' europeo[29]. Un doppio binario che sembra rivelare un margine di tutela più ampio possibile che passa attraverso la valorizzazione del ruolo delle autorità indipendenti e del diritto a un ricorso effettivo tutelato dall'art. 47 della Carta.

La manipolazione rispetto all'annullamento della decisione si apprezza

[27] Punto 56.
[28] Cfr. il punto 64.
[29] Così al punto 65.

dunque non solo con riferimento ai soli artt. 7 e 8 della Carta, ma anche grazie all'attenzione che la Corte dedica alla previsione affidata all'art. 47 che tutela il diritto a un ricorso effettivo innanzi a un giudice imparziale.

3. Dall'adeguatezza alla sostanziale equivalenza. Da mihi data, cetera tolle

Il momento in cui tuttavia diviene più evidente l'operazione complessiva condotta dalla Corte di giustizia, insieme alle forzature che essa inevitabilmente implica, è quello relativo al giudizio sul rispetto delle condizioni previste dalla direttiva 95/46/CE per la legittimità della decisione della Commissione. In tale ambito, compito della Corte diviene quello di condurre uno scrutinio sul livello di adeguatezza della tutela offerta dall'ordinamento statunitense.

Il punto che maggiormente si presta alla manipolazione interpretativa della Corte di giustizia è quello in cui i giudici osservano che, a ben vedere, la direttiva non individua in maniera esaustiva e analitica i criteri per valutare l'adeguatezza del livello di protezione offerto dall'ordinamento di un paese terzo. Né, aspetto ancora più rilevante, la nozione di adeguatezza è oggetto di specifica definizione. Al riguardo, infatti, l'art. 25, par. 2, si limita a stabilire che l'adeguatezza «è valutata con riguardo a tutte le circostanze relative a[d] un trasferimento o ad una categoria di trasferimenti di dati»; e, in secondo luogo, che «sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate». Questa indicazione, nondimeno, presenta tutt'altro che carattere esaustivo. In sintesi: non c'è riscontro di un concetto di adeguatezza espresso in senso vincolante, né di un set di criteri ai quali tale apprezzamento debba necessariamente essere informato.

La Corte al riguardo ammette che, al par. 6, l'art. 25 riferisce alla legislazione nazionale e agli eventuali impegni internazionali il giudizio di adeguatezza; e che, comunque, tale protezione deve essere valutata «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona». Proprio questo passaggio appare emblematico: sembra che lo stesso parametro di adeguatezza sia concepito come flessibile ed elastico, da interpretare alla luce dell'esigenza di tutela dei diritti fondamentali in gioco. La Corte, incorrendo in questo passaggio, sembra voler dare

sostanza alla nozione di adeguatezza quando invece, nei fatti, finisce per svuotarla di un significato preciso.

Nel punto successivo[30], poi, i giudici paiono confermare indirettamente questo sbilanciamento della Corte a favore di una tutela dei dati personali secondo un canone di equivalenza anziché di mera adeguatezza: questa sfumatura sembra emergere nell'enfasi data all'obiettivo dell'art. 25 della direttiva, vale a dire «assicurare […] la continuità del livello elevato di tutela di tale protezione in caso di trasferimento di dati personali verso un paese terzo» (nella versione in lingua inglese «*to ensure that the high level of that protection continues where personal data is transferred to a third country*»). Se certamente il ricorso terminologico alla nozione di continuità non può considerarsi dirimente rispetto alla pretesa differenza tra il significato di adeguatezza e quello di equivalenza, è tuttavia confessoria l'affermazione che denuncia l'obiettivo di un'ideale estensione territoriale extra-UE dell'applicazione delle garanzie previste dalla disciplina comunitaria.

La vera declinazione del parametro di adeguatezza secondo un'angolazione che lo parifica a quello di equivalenza si nota nel successivo passaggio in cui la Corte[31], pur premurandosi di precisare che lo standard di adeguatezza non implica un livello di protezione identico a quello europeo, richiamando le argomentazioni dell'Avvocato generale[32], specifica che il termine adeguatezza sottende l'esigenza di livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione –passaggio cruciale- «in forza della direttiva 95/46, letta alla luce della Carta». Ecco

[30] Cfr. il punto 72.

[31] Si v. il punto 73.

[32] Conclusioni dell'Avvocato generale Bot, 23 settembre 2015, C-362/14, *Maximillian Schrems v. Data Protection Commissioner*. In particolare, al punto 141, richiamato dalla Corte, così si esprime l'Avvocato generale: «un paese terzo assicura un livello di protezione adeguato solo qualora, al termine di una valutazione di insieme del diritto e della prassi nel paese terzo in questione, essa sia in grado di dimostrare che tale paese offre un livello di protezione sostanzialmente equivalente a quello offerto da tale direttiva, anche se le modalità di tale protezione possono essere diverse da quelle generalmente vigenti all'interno dell'Unione». Dunque, l'autore, o quantomeno l'artefice in prima battuta della manipolazione è piuttosto l'Avvocato generale. Che, non a caso, dopo essersi spinto così coraggiosamente in un argomento assai delicato, avverte, al successivo punto, l'esigenza di precisare che «[b]enché il termine inglese 'adequate' possa essere inteso, dal punto di vista linguistico, nel senso che esso designa un livello di protezione appena soddisfacente o sufficiente, e[d] avere pertanto un campo semantico diverso dal termine francese 'adéquat', si deve osservare che il solo criterio che deve guidare l'interpretazione di tale termine è l'obiettivo consistente nel conseguimento di un livello elevato di protezione dei diritti fondamentali, come richiesto dalla direttiva 95/46».

il preorientamento assiologico (o, se si volesse leggere maliziosamente, il pregiudizio assiologico) che conduce alla conversione del parametro di adeguatezza in quello di equivalenza tramite il trasformatore permanente della Carta dei diritti fondamentali: la Corte è chiara nell'esprimere l'avviso che è proprio una lettura teleologicamente ispirata dalla Carta a legittimare questa operazione di manipolazione della direttiva.

Si registra poi un'attenzione da parte della Corte alla natura dinamica del livello di protezione, che può variare a seconda di fattori diversi. Proprio per questo la Corte precisa che la Commissione è tenuta a effettuare una verifica periodica sull'adeguatezza della protezione in forza della direttiva. Siffatta verifica, aggiunge la Corte, è «in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo»[33]. E naturalmente, ai fini di tale verifica deve tenersi conto delle circostanze intervenute successivamente alla decisione della Commissione: ecco l'esigenza di una rivisitazione sul rispetto dello standard che la direttiva impone per assicurare quella continuità di protezione anche sotto il profilo temporale, e non meramente spaziale[34].

Al successivo punto 74 la sentenza fa emergere un ulteriore profilo di dinamizzazione, laddove la Corte precisa che gli strumenti di tutela scelti dai paesi terzi possono essere senz'altro differenti da quelli adottati negli Stati membri per ottemperare ai requisiti della direttiva «letta alla luce della

[33] Cfr. il punto 78.

[34] Si coglie in questo atteggiamento l'influenza esercitata, ancora una volta, dal parere dell'Avvocato generale, che ai punti 146 e ss. precisa: «al fine di assicurare l'effetto utile dell'articolo 25, paragrafi da 1 a 3, della direttiva 95/46, occorre tenere conto del fatto che l'adeguatezza del livello di protezione offerto da un paese terzo costituisce una situazione evolutiva che può mutare nel tempo in funzione di una serie di fattori. Gli Stati membri e la Commissione devono pertanto essere costantemente attenti ad ogni mutamento di circostanze idoneo a rendere necessaria una rivalutazione dell'adeguatezza del livello di protezione offerto da un paese terzo. Una valutazione dell'adeguatezza di tale livello di protezione non può affatto essere fissata a[d] un momento determinato e, poi, essere mantenuta indefinitamente, a prescindere da qualsiasi mutamento di circostanze che mostri che, in realtà, il livello di protezione offerto non è più adeguato. L'obbligo del paese terzo di assicurare un livello di protezione adeguato costituisce pertanto un obbligo di durata. Pur se la valutazione è effettuata in un momento determinato, il mantenimento della decisione di adeguatezza presuppone che nessuna circostanza intervenuta successivamente sia in grado di rimettere in discussione la valutazione iniziale effettuata dalla Commissione. Infatti, non si deve perdere di vista il fatto che l'obiettivo dell'articolo 25 della direttiva 95/46 consiste nell'evitare che i dati personali vengano trasferiti verso un paese terzo che non assicura un livello di protezione adeguato, in violazione del diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta».

Carta». Si intravede in questo passaggio un'ulteriore traccia dell'itinerario di manipolazione che percorre l'intera architettura della sentenza: non è più la direttiva la sola base giuridica cui ancorare la valutazione di legittimità e di conformità all'*acquis* europeo della decisione della Commissione, ma quest'ultima si allarga alla Carta dei diritti fondamentali, che entra sulla scena con la sua portata 'costituzionalizzatrice' e rende evidente il percorso da una protezione perlopiù mercantilistica della circolazione dei dati personali a una *fundamental rights oriented*.

Il punto è strategico per la Corte per riaffermare che gli strumenti adottati da paesi terzi devono rivelarsi efficaci ad assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione.

L'approccio dei giudici del Lussemburgo sembra peculiare a questo riguardo.

Da un lato, infatti, la Corte fa esplicitamente ammissione della diversità degli strumenti che possono assicurare, in paesi terzi, la tutela dei dati personali secondo standard adeguati, se comparati al livello di protezione dell'Unione europea. Sembrerebbe dunque un passo indietro, una sorta di *self-restraint* della Corte che prende atto che al (quasi) medesimo risultato è possibile pervenire tramite un percorso diverso, così ponendo le basi, concettualmente, per una sostanziale insindacabilità delle soluzioni normative adottate in ordinamenti diversi da quello dell'Unione europea.

Dall'altro lato, però, la Corte entra eccome nel merito degli strumenti normativi che assicurano la protezione dei dati personali nell'ordinamento cui si riferisce la constatazione di adeguatezza contenuta nella decisione 2000/520, ossia quello statunitense. E lo fa con un approccio che è inedito, almeno per quanto riguarda le decisioni che più direttamente vertono in materia di diritti fondamentali, e non di libertà economiche: con uno sguardo pragmatico e un'attenzione particolare per il soddisfacimento dell'obiettivo di tutela sotteso alle misure in questione. Proprio al punto 74, infatti, si rileva come, a dispetto della loro possibile diversità rispetto a quelli impiegati dagli Stati membri, tali strumenti devono rivelarsi efficaci 'nella prassi' al fine di assicurare una protezione 'sostanzialmente equivalente' (importante manipolazione del dato normativo) a quella garantita all'interno dell'Unione europea. E da questo rilievo prende avvio l'esame che la Corte successivamente svolge, con grande taglio pratico, sulle misure previste dall'ordinamento statunitense e segnatamente del sistema di *Safe Harbor*, al fine di verificare se queste ultime corrispondano al requisito di una protezione equivalente. In questo modo, l'indagine pragmaticamente condotta dai giudici sulle garanzie previste negli Stati

Uniti permette di apprezzare, alla stregua di un parametro interposto, la sostanziale divergenza di questo ordinamento rispetto agli standard individuati dalla direttiva, divergenza che vale a invalidare la decisione della Commissione che, al contrario, ne aveva constatata l'adeguatezza. Ma è una verifica, quella svolta dalla Corte di giustizia, che per quanto formalmente risponda a un confronto tra il contenuto della decisione e i requisiti della direttiva, nella sua valenza pratica si risolve in uno scrutinio sulla conformità delle disposizioni rilevanti vigenti negli Stati Uniti alle norme della Carta che tutelano i diritti fondamentali interessati (tutela della vita privata e familiare, tutela dei dati personali, diritto a un giusto processo).

4. Libertà economiche vs diritti fondamentali. L'approccio evolutivo della Corte di giustizia da un intermediate *a uno* strict scrutiny

Un fattore che si è rivelato decisivo nell'economia della decisione della Corte di giustizia riposa certamente sul preorientamento assiologico che si coglie nelle parole dei giudici laddove occorre procedere a bilanciare diritti fondamentali e libertà economiche. Un preorientamento di cui emergeva traccia evidente già nella decisione *Google Spain,* e in special modo in due frangenti[35].

In primo luogo, laddove la Corte di giustizia espressamente aveva riconosciuto, al punto 97, che i diritti fondamentali derivanti dagli artt. 7 e 8 della Carta fossero destinati a prevalere, in linea di principio, sull'interesse economico, nella fattispecie, del gestore del motore di ricerca.

In secondo luogo, questo atteggiamento si coglieva nell'omissione di qualsiasi riferimento esplicito alla libertà di espressione, senz'altro attinta dall'esito della pronuncia della Corte di giustizia e interessata dall'opera di bilanciamento ivi condotta, sebbene uscitane soccombente. Questo dato appare emblematico di un'opera di (s)bilanciamento svolta secondo un preciso orientamento, incline a riconoscere una portata estensiva e ampia ai diritti alla privacy e alla tutela dei dati personali.

Questa impostazione sembrerebbe tuttavia poco rispettosa dell'approccio che la Carta dei diritti fondamentali dell'Unione europea fa suo, collocando i diritti allo stesso livello, secondo un catalogo assiologico che

[35] Sia consentito richiamare, a proposito della manipolazione che la Corte di giustizia aveva compiuto nel caso *Google Spain*, O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo?*, cit. e Id., *Interpretazione o manipolazione?,* cit.

non conosce differenziazioni e gerarchie ma che concepisce la possibilità di realizzare operazioni di bilanciamento, purché ne riesca tutelato il contenuto essenziale del diritto sottoposto a sacrificio[36].

Di questa operazione, che recupera spazio ai diritti fondamentali della sfera della riservatezza con sacrificio delle libertà che riguardano la sfera economica, si trova piena conferma anche nell'impianto della pronuncia resa nel caso *Schrems.* Al punto 48, in particolare, la Corte osserva che la direttiva 95/46/CE, nel regolare il trasferimento di dati personali verso paesi terzi, ne riconosce la necessità ai fini degli scambi internazionali. Non è un richiamo puramente formale o simbolico, perché quella della Corte sembra una presa d'atto della natura strategica che i trasferimenti di dati fuori dall'Unione europea rivestono, con conseguenze che toccano anche le libertà fondamentali di natura economica sancite dai trattati.

Anzi, la successiva indagine compiuta dai giudici al fine di accertare il funzionamento del meccanismo del *Safe Harbor* rivela un'inedita capacità della Corte di 'calarsi' nella dimensione empirica e di condurre una verifica circa il concreto operare dei principi vigenti nell'ordinamento statunitense e le relative implicazioni non solo per la tutela dei dati personali ma anche per la libertà di impresa e di iniziativa economica che fa capo ai soggetti che nella maggior parte dei casi trasferiscono dati personali da/per l'Unione europea.

La Corte però, sempre al punto 48, pone un paletto molto chiaro: i trasferimenti in questione non possono avere luogo se non in presenza di un livello di protezione adeguato.

Così, le ragioni del commercio non possono mai prevalere su quelle della privacy, se non in presenza di requisiti particolari. Sembra confermata la linea già intrapresa nella sentenza *Google Spain*, dove i diritti 'economici' soccombono rispetto alla privacy[37].

[36] Cfr. l'art. 52 della Carta dei diritti fondamentali dell'Unione europea.

[37] In questa pronuncia, diversi erano i profili dai quali emergeva la netta prevalenza, da un punto di vista assiologico, dei diritti fondamentali rispetto alle libertà economiche. La prima fondamentale anomalia argomentativa riguarda la mancanza di riferimenti espliciti all'art. 16 della Carta, che tutela la libertà di impresa, a dispetto delle numerosissime citazioni che hanno per protagonisti gli artt. 7 e 8 della Carta. Per vero, analogo destino accomuna la libertà di espressione, tutelata dall'art. 11, diritto fondamentale anch'esso attinto dalla sentenza *Google Spain* ma che trova scarsissimo peso nell'argomentazione della Corte. Il secondo elemento su cui riposa la superiore considerazione che i giudici di Lussemburgo nutrono dei diritti alla privacy e alla protezione dei dati personali rispetto ai diritti della sfera economica corrisponde all'ammissione esplicita che la stessa Corte compie, al punto 97, dove ricorda che i diritti tutelati dagli artt. 7 e 8 «prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca,

Che una simile impostazione, già emersa in *Google Spain*, sia confermata dall'argomentazione della Corte di giustizia nella pronuncia in commento appare un dato assai curioso, che parzialmente sembra rivelare un'eterogenesi dei fini. La Corte di giustizia, infatti, giudice di un ordinamento nato per la creazione di un mercato unico e avulso rispetto al tema dei diritti fondamentali, di cui il diritto dell'Unione europea faceva esperienza soltanto come possibili motivi legittimi di restrizione, da parte degli Stati membri, delle libertà economiche (e dunque come eccezioni a queste ultime), compie una netta inversione: divenendo, di fatto, giudice delle ragioni dei diritti fondamentali davanti ai quali soccombono ora i diritti 'economici' per la cui protezione quell'ordinamento era stato concepito.

In questo modo, però, la Corte introduce un criterio di differenziazione nelle operazioni di bilanciamento che non trova riscontro nel documento che è oggetto specifico di *enforcement*, vale a dire la Carta dei diritti fondamentali dell'Unione europea. Come noto, infatti, tale atto non colloca i diritti in una scala gerarchica, né assicura alcuna prevalenza assiologica a beneficio di alcune categorie di diritti a scapito di altre[38].

Questo nuovo equilibrio, che però sembra negare per certi versi il disegno complessivo della Carta di Nizza, consente di rendere meno brusco e problematico il passaggio che conduce la Corte a innalzare il parametro di adeguatezza stabilito dalla direttiva in uno di sostanziale equivalenza.

Su questo terreno, rispetto all'operazione complessiva di innalzamento del livello interno di tutela dei diritti fondamentali, si devo però registrare l'intervento di due variabili a carattere dinamico che sembrerebbero condurre verso esiti opposti.

La prima variabile corrisponde a un elemento non nuovo, ossia la tendenza a compiere un'inversione temporale nell'interpretazione del rapporto tra disposizioni della Carta e disposizioni della direttiva 95/46/CE[39]. Confermando un indirizzo già rintracciabile nella sentenza *Google Spain*, la Corte di giustizia[40] afferma che è l'art. 25, par. 6, della direttiva ad attuare l'obbligo esplicito di protezione dei dati personali previsto dall'art.

---

ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona». In proposito, v. O. Pollicino, *Interpretazione o manipolazione?*, cit., 17 ss.

[38] Sulla sistematica della Carta e sui problemi che essa racchiude, cfr. G.F. Ferrari, *Le libertà. Profili comparatistici*, Milano, 2011, spec. 290 ss.

[39] Di questa attitudine a un capovolgimento temporale si era già parlato, a proposito della sentenza *Google Spain,* in O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo?,* cit., 14 ss.

[40] Cfr. il punto 72.

8, par. 1, della Carta. Nella sentenza del maggio 2014, invece[41], la Corte del Lussemburgo aveva rilevato come fosse un gruppo di disposizioni racchiuse nella direttiva a recepire e attuare le prescrizioni contenute negli artt. 7 e 8 della Carta.

Non si può certo negare che, collocandosi la Carta e le disposizioni della direttiva in un diverso rango nel diritto dell'Unione europea, e rispettivamente a livello primario e derivato, sussista tra le medesime fonti un rapporto assimilabile a quello che intercorre tra norme di principio e norme prescrittive. Nondimeno, e l'anomalia del costrutto ordinamentale comunitario insiste proprio qui, solo un'inversione di carattere temporale, come quella operata dalla Corte, consente di recuperare un siffatto rapporto nella fattispecie, a fronte di una normativa per così dire 'di dettaglio' (quella appunto della direttiva) risalente a cinque anni prima dell'adozione (allora non ancora vincolante) della Carta.

Da questa aporia è possibile uscire soltanto ammettendo che la Corte abbia compiuto, come nel caso *Google Spain*, un'evidente forzatura, vicina a una manipolazione, volta a favorire l'espansione della tutela del diritto fondamentale alla privacy[42]: e del resto, è chiaro che nella mente del legislatore della direttiva non potesse certo albergare alcuna *ratio* attuativa di principi che ancora non erano stati enunciati, almeno formalmente, nell'ordinamento europeo. Vero è, naturalmente, che il rispetto della vita privata e familiare, valori sanciti dall'art. 8 della Convenzione europea dei diritti dell'uomo («CEDU»), già costituivano parte del patrimonio comunitario tramite il filtro delle tradizioni costituzionali degli Stati membri e in quanto principi generali, secondo il disposto dell'art. 6, par. 2, del TUE[43]. Nondimeno, se anche si volesse intendere le disposizioni della

[41] Corte di giustizia UE, 13 maggio 2014, cit., punto 69.

[42] Questa amplificazione del portato dei diritti tutelati dagli artt. 7 e 8 della Carta aveva però trovato un contrappeso nell'argomentazione della Corte di giustizia, che era stata costretta, con quella che non si è esitato a definire una *excusatio non petita,* a sposare un'interpretazione ampia della nozione di titolare del trattamento (cui ricondurre i relativi obblighi previsti dalla direttiva 95/46), nozione prevalentemente di carattere tecnico, giustificando tale scelta sull'assunto che una diversa interpretazione si sarebbe rivelata contraria alla lettera e alla finalità dell'art. 2 della direttiva, intesa ad assicurare una tutela efficace e completa delle persone interessate. Si v. il punto 34, e nuovamente, O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo?,* cit., 17-18. Sia inoltre consentito rinviare anche a M. Bassini-O. Pollicino, *Bowling for Columbine. La Corte di giustizia sul caso Google Spain: l'oblio (quasi) prima di tutto?,* in www.diritto24.ilsole24ore.it, 13 maggio 2014.

[43] Non è inutile rinviare, per i profili generali, agli scritti di A. Ruggeri, *Crisi dello Stato nazionale, dialogo intergiurisprudenziale, tutela dei diritti fondamentali: notazioni introduttive*, in www.giurcost.org, 22 novembre 2014; Id., *Maggiore o minor tutela*

direttiva come attuative di prescrizioni allora contenute soltanto nella CEDU, e poi riprodotte dalle corrispondenti disposizioni della Carta, si dovrebbe comunque rispondere a due obiezioni.

La prima: questa lettura non supera il problema dell'inversione temporale, stante l'approccio formalistico della Corte di giustizia che fa espressamente riferimento alle disposizioni della direttiva come attuative delle previsioni della Carta.

La seconda: la Carta descrive –almeno da un punto di vista formale- una protezione assai più ampia e articolata rispetto agli enunciati della CEDU[44], declinando la tutela sia sul versante della vita privata e familiare, sia su quello della protezione dei dati personali.

Vi è poi un'ulteriore variabile da prendere in considerazione, che emerge dal punto 76 della decisione, laddove la Corte esplicita –come si è ricordato- che è compito della Commissione condurre una verifica periodica sull'adeguatezza del livello di protezione assicurato in un paese terzo in funzione all'evoluzione cui esso può essere soggetto. Si introduce

nel prossimo futuro per i diritti fondamentali?, in www.giurcost.org, 2015, 1, 34 ss.; A. Guazzarotti, *I diritti fondamentali dopo Lisbona e la confusione del sistema delle foni,* in *Rivista AIC,* 2011, 3 ss.; e, sul tema delle tradizionali costituzionali, *ex multis,* P. Ridola, *La Carta dei diritti fondamentali dell'Unione Europea e le «tradizioni costituzionali comuni»degli stati membri,* in Id., *Diritto comparato e diritto costituzionale europeo*, Torino, 2010, 163 ss.; S. Ninatti*, Ieri e oggi delle tradizioni costituzionali comuni: le novità nella giurisprudenza comunitaria*, in G. D'Elia-G. Tiberi-M.P. Viviani Schlein (a cura di), *Scritti in memoria di Alessandra Concaro,* Milano, 2012, 533 ss.; G. de Vergottini, *Tradizioni costituzionali comuni e Costituzione europea*, in www.forumcostituzionale.it, 8 novembre 2014; A. Ruggeri, *«Tradizioni costituzionali comuni» e 'controlimiti', tra teoria delle fonti e teoria dell'interpretazione*, in *DPCE*, 2003, 1, 101 ss.; V. Sciarabba, *Tra fonti e corti. Diritti e principi fondamentali in Europa: profili costituzionali e comparati degli sviluppi sovranazionali*, Padova, 2008. G. Cozzolino, *Le tradizioni costituzionali comuni nella giurisprudenza della Corte di giustizia delle Comunità europee*, in P. Falzea-A. Spadaro-L. Ventura (a cura di), *La Corte costituzionale e le corti d'Europa*, Torino, 2003, 3 ss.. Sia consentito altresì rinviare a O. Pollicino, *Corte di giustizia e giudici nazionali: il moto 'ascendente', ovverosia l'incidenza delle «tradizioni costituzionali comuni» nella tutela apprestata ai diritti dalla Corte dell'Unione,* in www.giurcost.org, 2015, 1, 242 ss.

[44] Non solo, evidentemente, la tutela è declinata all'interno della Carta in due diverse disposizioni che fotografano l'aspetto negativo e quello positivo del diritto, rispettivamente, alla privacy e alla protezione dei dati personali: come nota T. Groppi, op. cit., il contenuto dell'art. 7 della Carta si differenzia dall'art. 8 CEDU per due aspetti. *In primis* la norma della Carta definisce il proprio ambito di applicazione con riferimento non già al rispetto della «corrispondenza», bensì più in generale alle «comunicazioni». In secondo luogo, l'art. 8 CEDU regola anche i limiti e le ingerenze da parte delle autorità pubbliche nell'esercizio di tale diritto, mentre l'art. 7 della Carta tace, non riproducendo il par. 2 dell'art. 8 CEDU, sulle possibili restrizioni, sulle quali si esprime comunque, in via generale e indifferenziata, l'art. 52.

così un elemento di dinamizzazione della protezione dai dati personali, che osta a una visione statica.

Viene da domandarsi, a questo riguardo, se davvero la Corte di giustizia e la Commissione si trovino di fronte a un'evoluzione del livello di tutela previsto nel paese terzo interessato, vale a dire gli Stati Uniti, o piuttosto a un'involuzione 'interna' all'Unione europea cui la Corte reagisce con fermezza, nel tentativo di recupero di un margine 'adeguato' di tutela comunitario partendo proprio dal blocco del trasferimento verso paesi terzi. D'altro canto, il giudizio sul livello di tutela offerto da un paese terzo si riflette sulla sorte (e sul potenziale pregiudizio) cui risultano esposti i dati personali degli interessati all'interno dell'Unione europea. È quindi ragionevole immaginare un'intima connessione fra l'interna 'involuzione' che, specie alla luce della più recente attualità, vede protagonista il diritto alla privacy e la connessa tutela dei dati personali, e il giudizio che la Commissione in prima battuta e, in sede di *review*, la Corte di giustizia sono chiamate a esprimere.

Se questa seconda variabile contribuisce all'affermazione di una concezione dinamica della tutela della privacy e dei dati personali, essa porta con sé due ricadute assai significative.

Per un verso, il novero dei fattori di cui la Commissione deve avere cognizione nell'esprimere una constatazione sull'adeguatezza della tutela offerta da un paese terzo è senz'altro ampio. Come detto, infatti, la Commissione non dovrà limitarsi a un accertamento iniziale ma, prendendo atto della possibile evoluzione del livello di protezione, sarà tenuta a verificare periodicamente il rispetto di quel parametro, rilevando eventuali scostamenti. Il che implica la capacità, da parte della Commissione, di riconoscere il mutamento di condizioni endogene ed esogene di sistema, fino alla possibilità di revocare, così revisionandola, una precedente valutazione di adeguatezza. Non solo: la pronuncia precisa che tale verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo. Sebbene questo inciso appaia tutt'altro che cristallino, lasciando sospesa la definizione delle condizioni che legittimano una doverosità all'azione della Commissione, esso rafforza l'idea di dinamicità e di ampio respiro della valutazione.

La Corte di giustizia, beninteso, riferisce la possibile evoluzione del livello di protezione al paese terzo verso il quale i trasferimenti di dati personali hanno luogo. Ciò non basta a escludere, tuttavia, che l'apprezzamento da parte della Commissione possa fondarsi anche su elementi endogeni, vale a dire sul livello di protezione all'interno dell'Unione euro-

pea[45]. In questo senso, il potere della Commissione di valutare l'adeguatezza del livello di protezione, non estraneo anche da fattori di carattere politico, consentirebbe un innalzamento delle 'difese immunitarie' dell'ordinamento europeo di fronte a circostanze interne che potrebbero incidere sulla protezione effettiva e secondo standard elevati della privacy e dei dati personali. A legittimare questa operazione pare essere la stessa Corte, che al punto 77 rievoca le parole dell'Avvocato generale sulla necessità di tenere conto anche delle circostanze intervenute successivamente all'adozione della decisione, così relativizzando al massimo grado ogni constatazione da parte della Commissione sull'adeguatezza della protezione offerta da un paese terzo[46].

Per altro verso, la dinamizzazione del giudizio di equivalenza apre a una riconsiderazione che non può che favorire l'innalzamento della tutela dei diritti in questione e passa attraverso l'affermazione per cui il margine di manovra della Commissione, chiamata ad apprezzare l'adeguatezza (*rectius*: sostanziale equivalenza) della tutela offerta da un paese terzo, diviene per forza di cose ridotto.

[45] D'altro canto, viene da chiedersi come potrebbe reagire la Corte di giustizia (e, dunque, come dovrebbe agire la Commissione) nell'ipotesi di un innalzamento 'interno' all'Unione europea del livello di tutela della privacy e dei dati personali, con riguardo alla valutazione da compiere sull'adeguatezza delle tutele offerte dall'ordinamento statunitense. Per effetto della manipolazione portata a termine nella sentenza *Schrems*, infatti, il parametro, prima flessibile e malleabile dell'adeguatezza viene trasformato in un più rigido vincolo di sostanziale equivalenza. L'irrigidirsi del canone al quale informare la verifica di legittimità del trasferimento dei dati verso gli Stati Uniti interroga dunque sulle conseguenze di una simile opzione: l'esigenza di rispettare il criterio di sostanziale equivalenza impone un continuo adeguamento, con una possibile 'corsa al rialzo', da parte dell'ordinamento statunitense? Quest'ultimo esito appare difficilmente realizzabile in termini empirici e rivela l'intento ideologico sotteso alla decisione della Corte di giustizia, che, nel tentativo di compiere un avanzamento nella qualità della tutela della privacy e dai dati personali, sembra, non si capisce quanto volontariamente, poter legittimare, almeno formalmente, un risultato difficilmente accettabile.

[46] Così le Conclusioni dell'Avvocato generale, cit., ai punti 137-138: «Tenuto conto della natura particolare della decisione di adeguatezza, quest'ultima deve essere oggetto di un riesame regolare da parte della Commissione. Se, a seguito di nuovi eventi verificatisi nel frattempo, la Commissione non modifica la propria decisione, essa conferma implicitamente, ma inevitabilmente, la valutazione effettuata all'inizio. Essa ribadisce pertanto la sua constatazione secondo la quale il paese terzo di cui trattasi assicura un livello di protezione adeguato ai dati personali trasferiti. Spetta alla Corte esaminare se tale constatazione continui ad essere valida malgrado le circostanze intervenute successivamente. Al fine di assicurare un controllo giurisdizionale effettivo su questo tipo di decisione, la valutazione della sua validità deve pertanto essere effettuata, a mio avviso, tenendo conto del contesto di fatto e di diritto attuale».

In questo frangente prende corpo l'idea di un processo di *judicial cross-fertilization* che potrebbe aver investito il ragionamento della Corte di giustizia nella ponderazione fra interessi di diverso peso, seppure di eguale forma e veste giuridica.

Sembra qui ritrovarsi, infatti, quell'atteggiamento della giurisprudenza della Corte suprema statunitense che aveva trovato la sua massima epifania nella celebre *footnote 4* alla sentenza *Carolene Products*[47]. Questo approccio tende a discriminare la tipologia di scrutinio sulla costituzionalità delle leggi a seconda che si tratti di normativa in materia economica o meno. Nel caso di disposizioni che attengono alla materia economica opererebbe una *presumption of constitutionality*, sicché il test da adottare al fine di verificare la compatibilità della legge di volta in volta interessata corrisponde a una *rationale basis review* che si colloca su un livello meno severo rispetto alla *strict scrutiny* cui sono invece soggette le leggi che attingono la materia delle libertà fondamentali. Questa dinamica appare riprodursi nel percorso tracciato dalla Corte di giustizia, che da comparto normativo a vocazione mercantilistica è passata a considerare la direttiva 95/46/CE (*medio* la decisione 2000/520) come un atto che incide direttamente su libertà fondamentali; così convertendo il proprio standard di *review* da un controllo 'intermedio', più simile al *rationale basis review* di stampo statunitense, a uno rigoroso, più vicino allo *strict scrutiny*. Questo mutamento di approccio vede come leva e protagonista assoluta la Carta, che permette, ma per altri versi obbliga a riconciliare con una cornice a tutela dei diritti fondamentali disposizioni introdotte quando l'ordinamento dell'Unione europea ne era di fatto ancora sguarnito.

Così, una legislazione basata sull'esigenza di favorire le libertà economiche (garantendo la circolazione dei dati personali, considerati un fondamentale *asset* a tale riguardo), il cui impatto sui diritti fondamentali non era dapprima apprezzato, appare ora annoverata nell'ambito della «*non-economic* legislation», che incidendo direttamente su diritti fondamentali impone un controllo rigoroso sul loro rispetto. Ne deriva l'esigenza che la Commissione, in sede di prima valutazione, e la Corte di giustizia, in sede di eventuale sindacato, procedano alla ponderazione degli interessi coinvolti secondo uno *strict scrutiny*; questo è l'esito della sentenza della Corte, che al punto 78 precisa appunto la necessità di effettuare un «controllo stretto» dei requisiti risultanti dall'art. 25 della direttiva, letto alla luce della Carta: ecco l'influenza 'manipolativa'.

[47] *United States v. Carolene Products Company*, 304 U.S. 144 (1938).

5. Da Digital Rights Ireland *a* Schrems*, ovvero dalla mancanza di proporzionalità alla violazione del contenuto essenziale*

Come è stato già sottolineato altrove[48], è piuttosto infrequente che i giudici della Corte di Lussemburgo, nel valutare l'incisione di norme di diritto derivato sui diritti fondamentali tutelati dalla Carta, si concentrino separatamente sui due profili che emergono dall'art. 52, par. 1, vale a dire la violazione del contenuto essenziale e la proporzionalità delle limitazioni.

A questa attitudine consolidata ha fatto eccezione, non senza passare inosservata[49], la pronuncia che la Corte ha restituito nel caso *Digital Rights Ireland* dell'aprile 2014, che ha inaugurato il trittico di decisioni relative al nuovo diritto alla privacy digitale.

In questa decisione, infatti, i giudici avevano distinto tra i due profili. Rilevando, da un lato, come la direttiva 2006/24/CE non importasse alcuna violazione del contenuto essenziale dei diritti sanciti dagli artt. 7 e 8 della Carta; e, dall'altro lato, come le misure dettate dalla medesima direttiva, tuttavia, non rispettassero il criterio di proporzionalità stabilito dall'art. 52, par. 1[50].

La sentenza *Schrems,* se letta in controluce con la tendenza ora descritta, restituisce invece uno spaccato diverso, nel quale l'argomentazione della Corte fa sì che nel pervenire a una declaratoria di annullamento della decisione 2000/520 della Commissione la violazione del contenuto essenziale dei diritti di cui agli artt. 7, 8 e 47 della Carta sia addebitata non tanto alla direttiva 95/46/CE, né alla decisione della Commissione che ha omologato gli standard di protezione di quel sistema, quanto piuttosto all'ordinamento statunitense.

Sullo sfondo di questa vicenda, e più in generale degli sforzi recenti della Corte di giustizia, si colloca indubbiamente la problematica della sorveglianza globale, destinata a tornare ciclicamente di prepotente attualità[51]. Il tutto con le implicazioni di carattere politico che ciò comporta.

---

[48] Si v. ancora O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo?,* cit, 13.

[49] Ivi.

[50] Giova richiamarne il contenuto: «Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

[51] Sul punto v. in questo Volume G. Resta, *La sorveglianza di massa e il conflitto*

Così, collegando la sentenza di ottobre con la pronuncia che aveva inaugurato il trittico di sentenze, vale a dire quella in materia di *data retention*, sembra potersi cogliere un *climax* di attenzione e di severità di giudizio da parte dei giudici di Lussemburgo, complici probabilmente anche i condizionamenti derivanti dallo scandalo NSA.

Questo atteggiamento emerge se si osserva il modo in cui la Corte di giustizia ha fatto applicazione, nei due casi, in modo opposto, dell'art. 52 della Carta al fine di verificare la legittimità delle limitazioni cui i diritti fondamentali in questione erano sottoposti.

In un primo momento, infatti, nel caso *Digital Rights Ireland,* la Corte di giustizia è stata chiamata a risolvere la questione su un piano meramente interno, valutando l'impatto della direttiva in materia di conservazione dei dati di traffico sui diritti fondamentali. E, nel tentativo di «lavare i panni sporchi in casa», la Corte si è concentrata sul profilo della proporzionalità, dato che il contenuto delle comunicazioni non era stato attinto dalle misure previste dalla direttiva e che quindi non poteva affermarsi una violazione del contenuto essenziale dei diritti di cui agli artt. 7 e 8 della Carta[52]. Quando invece si esercita sul sistema nordamericano del *Safe Harbor*, che costituisce il cuore della normativa e della prassi sulla protezione dei dati personali, la Corte di giustizia, agendo come se questo fosse l'oggetto del suo giudizio, perviene alla conclusione che lo stesso

regolatorio USA/UE, p. 697

[52] Cfr. Corte di giustizia UE, 8 aprile 2014, cit., ai punti 39-40: «[p]er quanto riguarda il contenuto essenziale del diritto fondamentale al rispetto della vita privata e degli altri diritti sanciti all'articolo 7 della Carta, si deve rilevare che, sebbene la conservazione dei dati imposta dalla direttiva 2006/24 costituisca un'ingerenza particolarmente grave in tali diritti, essa non è tale da pregiudicare il suddetto contenuto poiché, come deriva dall'articolo 1, paragrafo 2, della stessa direttiva, quest'ultima non permette di venire a conoscenza del contenuto delle comunicazioni elettroniche in quanto tale. Tale conservazione dei dati non è neppure idonea a pregiudicare il contenuto essenziale del diritto fondamentale alla protezione dei dati personali, sancito all'articolo 8 della Carta, considerato che la direttiva 2006/24 prevede, all'articolo 7, una regola relativa alla protezione e alla sicurezza dei dati ai sensi della quale, fatte salve le disposizioni adottate in conformità delle direttive 95/46 e 2002/58, i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione sono tenuti a rispettare taluni principi di protezione e di sicurezza dei dati, principi in base ai quali gli Stati membri assicurano l'adozione di adeguate misure tecniche e organizzative contro la distruzione accidentale o illecita, la perdita o l'alterazione accidentale dei dati». Come si nota, curiosamente nella sentenza *Digital Rights Ireland* la Corte di giustizia ha fatto oggetto gli artt. 7 e 8 di una considerazione non più unitaria, come era accaduto di sovente nella sua giurisprudenza, bensì distinta e separata, così da cogliere in modo maggiormente puntuale le implicazioni delle misure previste dalla direttiva, rispettivamente, sulla tutela della riservatezza e sulla protezione dei dati a carattere personale.

determina una violazione del contenuto essenziale dei diritti fondamentali racchiusi negli artt. 7, 8 e 47 della Carta. Traendo così dal precedente *Digital Rights Ireland* una giustificazione per un riscontro più invasivo rispetto a un sistema di sorveglianza che espone il diritto alla privacy a un equilibrio fragilissimo.

Questo giudizio, peraltro, sembra prescindere –almeno argomentativamente- dalla scelta, compiuta dalla Corte, di elevare il parametro di valutazione delle garanzie offerte dal sistema statunitense dalla mera adeguatezza alla sostanziale equivalenza. Secondo i giudici, in maniera molto netta, disposizioni come quelle vigenti nel sistema statunitense producono conseguenze per i dati personali trasferiti dall'Unione europea da cui deriva la violazione del contenuto essenziale dei diritti fondamentali tutelati dalla Carta. Naturalmente, una conclusione così netta preclude e assorbe alle origini ogni possibile velleità interpretativa legata al diverso (ma subordinato) profilo della mancanza di proporzionalità. Certo, rimane insoluto il quesito teorico per l'interprete sull'esito cui la Corte sarebbe potuta addivenire se il parametro di giudizio fosse stato manutenuto fedele alla lettera della direttiva, ossia in termini di 'adeguatezza' e non già di sostanziale equivalenza.

Il tema della sorveglianza globale, e delle reazioni che sul fronte legislativo si registrano, pone tuttavia una serie di quesiti.

Il primo è un problema di comunicazione o, meglio, di comunicabilità, e riguarda in particolar modo gli Stati Uniti.

Il secondo è un problema di resistenza, o per meglio dire di differenziazione insanabile con gli ordinari strumenti di armonizzazione vigenti all'interno dell'Unione europea.

Per quanto riguarda il primo punto, occorre prendere atto che se è vero che la sentenza *Schrems*, per quanto silente, rappresenta la reazione sulla sponda europea allo scandalo NSA, è altresì vero che la portata delle intromissioni nella privacy da parte delle autorità statunitensi appare oggi doversi ridimensionare, e nella fattispecie è stata probabilmente sopravvalutata o comunque sovradimensionata.

Da Oltreoceano, infatti, si intravedono alcuni primi, timidi segnali di un'inversione di rotta nel rapporto tra tutela della sicurezza nazionale e protezione della privacy e dei dati personali, testimoniati da due importanti episodi di recente attualità.

Lo scorso maggio, con la sentenza *ACLU v. Clapper*[53], la Court of Appeals for the Second Circuit ha stabilito che la Section 215 del Patriot

[53] *ACLU v. Clapper*, No. 14-42 (2d Cir. 2015).

Act non autorizza la NSA a compiere una raccolta di blocco dei metadati relativi alle utenze telefoniche su scala globale, così privando l'agenzia di sicurezza del governo statunitense della base giuridica per un intervento assai invasivo.

La vicenda, che ha tratto origine dalle rivelazioni di Edward Snowden, vedeva contrapposti la American Civil Liberties Union e la NSA, in persona del suo direttore James Clapper. Da un lato, la ACLU lamentava che un'operazione di sorveglianza globale come quella condotta della NSA rappresentasse un'interferenza rispetto al diritto alla riservatezza, nonché alla libertà di espressione. Inoltre, le misure di sorveglianza avrebbero costituito delle restrizioni non assistite dalle garanzie previste dal Quarto Emendamento. Dall'altro, la NSA opponeva che tali operazioni fossero pienamente consentite in base al disposto del Section 215 del Patriot Act.

La norma contenuta nel Section 215 del Patriot Act, come modificata nel corso del tempo, attribuiva all'FBI il potere di richiedere un ordine di esibizione di qualsiasi supporto materiale per acquisire a fini investigativi informazioni di sicurezza non riguardanti cittadini statunitensi o per la protezione da attività di terrorismo internazionale o di *intelligence* clandestina.

Tale disposizione conteneva al proprio interno una sorta di «expiration clause», e ha pertanto formato oggetto di diverse proroghe susseguitesi nel tempo, dal 31 dicembre 2005 (la data di *expiration* originaria) fino alla scadenza del 1 giugno 2015, quando il Senato ha rinunciato a estenderne nuovamente l'efficacia. In particolare, il Senato ha approvato l'USA Freedom Act[54] che interviene su diversi punti del Patriot Act ma non riconosce un analogo potere di raccolta di metadati con portata globale: la NSA e gli altri organismi di sicurezza potranno ottenere queste informazioni secondo un iter che contempla ora l'intervento dell'autorità giudiziaria.

Alla luce di questi sviluppi, bisogna forse interrogarsi se la frattura che in materia di tutela dei dati personali separa la sensibilità statunitense da quella europea sia ancora così ampia o se, invece, gli accadimenti più recenti non restituiscano uno spaccato in cui le due visioni appaiono conciliarsi, o comunque avvicinarsi[55].

[54] Cfr. A. Yuhas, *NSA reform: USA Freedom Act passes first surveillance reform in decade – as it happened,* in *The Guardian,* 3 giugno 2015; C. Cohn-R. Reitman, *USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here,* 2 giugno 2015, in www.eff.org.

[55] Per un quadro generale di sistema a livello comparato, non è inutile rinviare a U. Pagallo, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Milano, 2008.

Chiaramente, analizzando a posteriori la sentenza della Corte di giustizia, sorge anche l'ulteriore quesito se i giudici di Lussemburgo non abbiano assimilato nella propria disamina, che comunque appare –come già ricordato- assai pragmatica rispetto al sistema di *Safe Harbor*, i cambiamenti ora ricordati. C'è forse un problema di comunicazione o di comunicabilità tra le due sponde dell'Oceano? Probabilmente sì, guardando alla più recente attualità. Quella stessa attualità che sembra documentare un'inversione dei ruoli, se si confrontano gli sviluppi descritti con la scelta della Francia, ad esempio, di sospendere la propria adesione alla CEDU[56].

Il secondo tema che si pone riguarda la difficoltà di conciliare con l'esigenza di standard comuni di tutela le scelte intestine dei singoli Stati membri prive di un ancoraggio nel diritto dell'Unione europea. La tutela dell'ordine pubblico e la protezione della sicurezza nazionale appartengono infatti a quella sfera entro la quale gli Stati membri conservano un'irripetibile discrezionalità legislativa ed è evidente come, pur nel rispetto delle disposizioni fissate dalla direttiva 95/46/CE, è ben possibile che gli Stati descrivano al loro interno un equilibrio diverso tra queste esigenze e la protezione dei dati personali, specie in settori non direttamente regolati dal diritto dell'Unione. In tale contesto, la Corte di giustizia sarebbe priva di poteri di intervento che consentano di riequilibrare l'assetto degli interessi rilevanti negli Stati membri.

Ancora, per rientrare nel perimetro del diritto dell'Unione europea, la direttiva, che allo stato definisce la cornice regolamentare in materia si differenzia da altri strumenti, fra cui il regolamento, in quanto affida agli Stati un margine di discrezione nell'attuazione degli obblighi di risultato che in essa vengono stabiliti. È indubbio che in queste circostanze possano darsi modalità di attuazione degli obblighi comunitari anche non coincidenti, con esiti di detrimento rispetto all'obiettivo di una effettiva armonizzazione.

Rimangono dunque, nell'ambito non regolato dal diritto dell'Unione europea così come in quello regolato, sacche di resistenza che possono tradursi in scelte normative che conducono a un livello di protezione frammentario tra gli Stati membri e, in definitiva, a una tutela a geometrie e confini variabili da stato a stato.

Un rimedio a questo secondo problema può rinvenirsi all'interno della Carta e dei Trattati; laddove, da un lato, come già si è ricordato, l'art. 6, par. 2, del TUE richiama la CEDU, annoverandola tra i principi generali

[56] *France informs Secretary General of Article 15 Derogation of the European Convention on Human Rights,* in www.coe.int, 25 novembre 2015.

del diritto comunitario e, dall'altro, l'art. 52, par. 3[57], della Carta stabilisce che ai diritti enunciati dalla Carta medesima corrispondenti a quelli sanciti dalla CEDU debbano attribuirsi significato e portata identici a quelli conferiti dalla Convenzione.

Queste disposizioni consentono di istituire un ponte, aprendo a una possibile conformazione esterna da parte della giurisprudenza della Corte europea dei diritti dell'uomo rispetto al sistema comunitario. E ciò sia perché è urgente la necessità, negli Stati membri, di provvedere a una rimodulazione della tutela dei valori in gioco, sia perché in parte le normative nazionali sfuggono all'ambito di applicazione del diritto dell'Unione europea.

Non è inutile, a questo riguardo, richiamare una recentissima presa di posizione della Corte di Strasburgo, che è stata espressa nella sentenza *Zakharov c. Russia*[58]. È tutt'altro che casuale che questa pronuncia sia stata definita il «follow-up» della Corte europea rispetto alla sentenza *Schrems* della Corte di giustizia[59]. La sua rilevanza, peraltro, è autoevidente, trattandosi della prima decisione pronunciata dopo i nuovi attacchi terroristici che hanno colpito la Francia.

Il caso riguardava un giornalista ed editore che aveva agito in giudizio sostenendo che le sue comunicazioni telefoniche fossero state oggetto di intercettazioni per finalità di prevenzione di attività terroristiche. Per effetto di un ordine governativo, infatti, gli operatori di telecomunicazioni erano stati obbligati a installare dispositivi volti a consentire la captazione

[57] Sul punto cfr. anche le sentenze della Corte di giustizia UE, 26 febbraio 2013, C-399/11, *Stefano Melloni c. Ministerio Fiscal* e 26 febbraio 2013, C-617/10, Åklagaren c. Hans Åkerberg Fransson. Per alcuni commenti, *ex multis* cfr. A. Ruggeri, *La Corte di giustizia e il bilanciamento mancato (a margine della sentenza Melloni),* in *Il Dir. dell'Unione europea,* 2013, 2, 399 ss.; M. Iacometti, *Il caso Melloni e l'interpretazione dell'art. 53 della Carta dei diritti fondamentali dell'Unione europea tra Corte di giustizia e Tribunale costituzionale spagnolo*, in *Rivista AIC,* 2013; G. De Amicis, *All'incrocio tra diritti fondamentali, mandato d'arresto europeo e decisioni contumaciali: la Corte di giustizia e il 'caso Melloni'*, in www.forumcostituzionale.it, 5 maggio 2013; F. Vecchio, *I casi Melloni e Akeberg: il sistema multilivello di protezione dei diritti fondamentali*, in *Quad. cost.,* 2013, 2, 454 ss.; R. Conti, *Gerarchia fra Corte di Giustizia e Carta di Nizza-Strasburgo? Il giudice nazionale (doganiere e ariete) alla ricerca dei 'confini' fra le Carte dei diritti dopo la sentenza Åklagaren (Corte Giust., Grande Sezione, 26 febbraio 2013, causa C-617/10),* in www.diritticomparati.it, 6 marzo 2013.

[58] Corte europea dei diritti dell'uomo, 4 dicembre 2015, *Roman Zakharov c. Russia*, n. 47143/06.

[59] P. De Hert-P. Cristobal Bocos, *Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment*, in www.strasbourgobservers.com, 23 dicembre 2015.

di comunicazioni da parte dell'agenzia di sicurezza nazionale in assenza di un provvedimento dell'autorità giudiziaria.

In entrambi i gradi di giudizio, tuttavia, l'editore era risultato soccombente dato che non era stato in grado di provare di aver effettivamente subito le conseguenze dell'implementazione di un sistema di sorveglianza di massa.

La *Grand Chamber*[60] ha ritenuto che nella fattispecie sussistesse una violazione del diritto sancito dall'art. 8 della CEDU.

Nel giungere alla sua decisione, la Corte di Strasburgo ha optato per la via che garantisse la tutela più ampia ai diritti fondamentali del ricorrente. La Corte europea, infatti, ha accertato la violazione dell'art. 8 della CEDU pur ammettendo che nella fattispecie non fosse stato provato che il ricorrente avesse subito un effettivo pregiudizio.

Prima ancora del merito della vicenda, dunque, era rilevante l'ammissibilità del ricorso, trattandosi di un caso nel quale non era contestata l'esistenza di un sistema di sorveglianza ma era indimostrato che il ricorrente ne avesse derivato detrimento alla propria riservatezza. Ancor più rilevante, a ben vedere, in considerazione della natura concreta del giudizio operato dai giudici di Strasburgo.

La Corte europea dei diritti dell'uomo ha parzialmente rivisitato il suo approccio rispetto alla casistica inerente all'implementazione di sistemi di sorveglianza, oscillante tra le decisioni che avevano ritenuto necessaria una ragionevole probabilità («reasonable likelihood») che le comunicazioni fossero state oggetto di intercettazione e quelle che, al contrario, consideravano sufficiente ai fini dell'ammissibilità del ricorso l'esistenza di una minaccia costituita da un sistema di sorveglianza.

I giudici di Strasburgo hanno per un verso fatto proprio quest'ultimo orientamento, espresso soprattutto nella sentenza *Klass*[61], così come reinterpretato nel caso *Kennedy*[62], laddove la Corte aveva convalidato questo standard di ammissibilità subordinandolo a due condizioni: esigendo, in primo luogo, che il ricorrente fosse tra i potenziali destinatari del sistema di sorveglianza in questione; e, in secondo luogo, l'assenza (o comunque la precarietà) di rimedi a disposizione dell'interessato. Secondo la sentenza *Kennedy,* è sufficiente che il ricorrente sia potenzialmente a rischio

[60] Per un commento, cfr. anche L. Woods, *Zakharov v Russia: Mass Surveillance and the European Court of Human Rights*, in www.eulawanalysis.blogspot.it, 16 dicembre 2015.
[61] Corte europea dei diritti dell'uomo, *Klass e altri c. Germania*, 6 settembre 1978, n. 5029/71.
[62] Corte europea dei diritti dell'uomo, *Kennedy c. Regno Unito*, 18 maggio 2010, n. 26839/05.

(«potentially at risk») affinché la sua domanda sia ammissibile davanti alla Corte. Questo standard supera così il test di *reasonable likelihood*, ampliando lo spazio di tutela dei ricorrenti vittime (effettive o non) di sistemi di sorveglianza di massa.

L'elemento dirimente della decisione nel caso *Zakharov,* dunque, è la prospettiva di una *individual justice* che la Corte di Strasburgo fa propria anche in assenza di un concreto, specifico pregiudizio per il ricorrente: l'esistenza di una minaccia di carattere massivo è sufficiente, nelle parole della Corte, per considerare violato il diritto alla riservatezza sancito dall'art. 8 della CEDU.

È muovendo da questa prospettiva, dunque, che la Corte di giustizia, e più in generale gli Stati membri e le istituzioni dell'Unione europea, potranno provvedere a quella rimodulazione della tutela dei dati personali che si impone come condizione di sistema, prima ancora di ogni garanzia esterna sul trasferimento verso paesi terzi.

Del resto, la pronuncia della Corte di Strasburgo sembra in consonanza con quella dell'omologa di Lussemburgo nel caso *Schrems:* in entrambi i casi, la valutazione della sussistenza di una violazione dei diritti fondamentali è risultata prescindere dalla dimostrazione di uno specifico e concreto pregiudizio per il ricorrente, fondandosi unicamente sulla constatazione di condizioni strutturali tali da compromettere il contenuto essenziale dei diritti in gioco.

Se però, sotto questo fronte, si coglie un'ideale continuità tra l'attività delle due Corti, sotto altro fronte occorre considerare che la sentenza nel caso *Zakharov* è destinata ad aprire, verosimilmente, una serie di ricorsi da parte dei cittadini dei vari stati contraenti che abbiano fatto luogo all'adozione di sistemi di sorveglianza, sospinti anche dall'onda emotiva del momento.

Sarà allora così che, smantellata (e da ricostruire) la decisione sul trasferimento verso gli Stati Uniti, gli Stati membri, a prescindere al campo di applicazione del diritto dell'Unione, potranno provvedere a quella rimodulazione della tutela dei dati personali che appare quanto mai necessaria come prima tappa per attribuire al principio di adeguatezza ormai convertito in equivalenza un contenuto che possa fungere da *tertium comparationis*.

6. L'ambito di applicazione territoriale formale e sostanziale

L'operazione compiuta dalla Corte di giustizia nella sentenza *Schrems* si segnala, peraltro, per una capacità di intervento che formalmente interessa soltanto il terreno dell'Unione europea ma sostanzialmente si rivela di portata globale.

I giudici di Lussemburgo, nella fattispecie, hanno sì dichiarato l'annullamento di una decisione adottata dalla Commissione europea sulla base delle disposizioni della direttiva 95/46/CE. Ma tale decisione, inerendo alle condizioni per la circolazione al di fuori dell'Unione europea dei dati personali, ha scatenato conseguenze ed effetti che non possono essere ridotti e non si esauriscono nel campo di azione del diritto dell'Unione.

Si tratta di una caratteristica non nuova, che descrive una dinamica di *cross-fertilization* già osservata nell'immediatezza della sentenza *Google Spain*. Anche in quel caso, infatti, la pronuncia della Corte aveva investito lo specifico contesto normativo della direttiva 95/46/CE, per evincerne l'esistenza di un diritto, per gli interessati, di ottenere dal gestore di motore di ricerca, in qualità di titolare del trattamento, la deindicizzazione dai risultati generati mediante l'uso di determinate parole chiave.

Come nel caso *Schrems*, però, le conseguenze che sono derivate dalla sentenza non sono rimaste circoscritte entro i confini europei, ma hanno investito lo scenario globale. Da un lato, non solo Google, diretto interessato, ma tutti i motori di ricerca hanno provveduto su scala globale (anche al di fuori dei confini europei) a predisporre sistemi di *take down* per riscontrare le richieste degli interessati. Dall'altro lato, pochi mesi dopo la sentenza della Corte di Lussemburgo, due corti canadesi, la Supreme Court of British Columbia[63] e la Court of Appeal[64], sono state messe di fronte alla richiesta di estendere a tutte le versioni nazionali dei motori di ricerca la rimozione dai risultati di ricerca operata dalla versione nazionale del servizio[65].

Conseguenze non dissimili, con effetti di *spillover,* si sono verificate anche a ridosso della pronuncia della Corte di giustizia del 6 ottobre. A distanza di breve tempo, infatti, la *Israeli Law, Information and Technology Authority* (ILITA), autorità di regolazione israeliana ha provveduto a revocare l'autorizzazione generale al trasferimento di dati personali verso gli Stati Uniti. Dunque, uno stato che non aderisce all'Unione europea (e

[63] *Equustek Solutions Inc. v. Jack,* 2014 BCSC 1063.
[64] *Equustek Solutions Inc. v. Google Inc*., 2015 BCCA 265.
[65] Si rinvia nuovamente a O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo?,* cit., 27

non è il solo[66]), Israele, ha di fatto recepito la sentenza della Corte di giustizia[67]. Le norme contenute nel *Privacy Protection Regulations, 2001* prevedono come eccezione al divieto di trasferimento di dati personali verso paesi terzi l'ipotesi in cui il paese di destinazione riceva dati personali dagli Stati membri dell'Unione europea in condizioni di equivalenza («under the same terms of acceptance»). Le autorità israeliane hanno dichiarato di aver fatto affidamento, a questo proposito, alla valutazione di adeguatezza del sistema dei *Safe Harbor* consolidata nella decisione 2000/250 della Commissione. Ora però, a fronte dell'annullamento della decisione suddetta, le stesse autorità hanno dichiarato di non poter più fondare su questa eccezione la legittimità del trasferimento di dati personali da Israele verso imprese stabilite negli Stati Uniti.

Dunque, un vero e proprio effetto domino che fa sì (nuovamente) che una pronuncia circoscritta all'ambito comunitario, anziché risolversi in questo specifico contesto, investa un campo d'azione più ampio, potenzialmente inesteso, che travolge ogni steccato o confine nazionale e sovranazionale.

È inevitabile osservare, da un punto di vista strettamente giuridico, che un simile effetto non sia privo di conseguenze sotto il profilo dell'impatto che esso produce rispetto al sistema interessato, quello statunitense. Non più chiamato a dar prova soltanto all'Unione europea di un avanzamento nel livello di tutela della privacy e dei dati personali, ma obbligato a compiere uno scatto più ampio, se non vorrà rimanere vittima di un isolamento che da madrepatria dei nuovi diritti e modello di democrazia moderna lo trasformi in territorio di frontiera per i diritti. Almeno per quelli in questione.

7. Il principio di equivalenza nella narrativa giurisprudenziale di Lussemburgo

Da ultimo, occorre cercare di comprendere come la pronuncia nel caso *Schrems* si possa riconciliare e riannodare alla narrativa, ormai ampia, della Corte di giustizia in tema di diritti fondamentali.

[66] Anche la Svizzera, che aveva adottato un accordo sul modello comunitario, il «US-Swiss Safe Harbor», ne ha sospeso l'attuazione fino a una nuova rinegoziazione con gli Stati Uniti. Si v. S. Crespi, *La tutela dei dati personali UE a seguito della sentenza Schrems,* in www.eurojus.it, 2 novembre 2015.

[67] Israeli Law, Information and Technology Authority, comunicato del 19 ottobre 2015.

Non può sfuggire, in primo luogo, un importantissimo richiamo che nelle maglie della pronuncia la Corte compie, riallacciandosi alla sentenza, o per meglio dire, alla saga *Kadi*[68].

Segnatamente, al punto 60 della sentenza, la Corte di giustizia esprime il principio per cui l'Unione europea, testualmente, è un'Unione di diritto, nel senso classico per cui «gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali». Questa precisazione serve ai giudici per puntualizzare, subito dopo, che le decisioni della Commissione adottate ai sensi dell'art. 25, par. 6, della direttiva 95/46/CE non possono sottrarsi a tale regola.

Leggendo la sentenza *Schrems* in controluce con la vicenda *Kadi*[69] si coglie l'immagine di un sistema europeo che risponde a un modello autonomo, un paradigma che in una costruzione dualistica non ammette forzature o restrizioni in materia di diritti fondamentali. Sembra potersi affermare che rispetto a ordinamenti diversi con cui il sistema giuridico europeo entra in comunicazione (e che impropriamente potremmo definire, da un punto di vista funzionale, il parametro interposto che attribuisce contenuto alle disposizioni dell'ordinamento comunitario) la tutela dei diritti fondamentali costituisce un baluardo invalicabile, un controlimite insuperabile di fronte al quale ogni norma o prassi di senso contrario riesce recessiva.

[68] Sono quattro le pronunce che appartengono alla saga *Kadi*: Tribunale CE, 21 settembre 2005, T-315/01, *Kadi c. Consiglio e Commissione;* Corte di giustizia UE, 3 settembre 2008, cause riunite C-402/05 P e C-415/05 P, *Yassin Abdullah Kadi e Al Barakaat International Foundation c. Consiglio dell'Unione europea e Commissione delle Comunità europee;* Tribunale CE, 30 settembre 2010, T-85/09, *Yassin Abdullah Kadi c. Commissione europea*; Corte di giustizia UE, 18 luglio 2013, cause riunite C-584/10 P, C-593/10 P e C-595/10 P, *Commissione europea e altri c. Yassin Abdullah Kadi*

[69] Per alcuni commenti, v. V. Sciarabba, *La Corte di giustizia, le misure antiterrorismo, i diritti fondamentali e la 'Carta di Nizza': l'epilogo della vicenda Kadi,* in *Forum di Quaderni Costituzionali,* 7 febbraio 2014; V. Sciarabba-O. Pollicino, *Lotta al terrorismo, diritti e principi fondamentali, rapporti tra ordinamenti: un importante capitolo della giurisprudenza* '*costituzionale*' *europea, in DPCE*, 2009, 1, 159; G.F. Ferrari, *Kadi: verso una Corte di giustizia costituzionale?, ivi* 187; R. Dickmann, *Il 'principio di legalità comunitaria' nel sindacato della Corte di giustizia delle Comunità europee degli atti comunitari esecutivi di risoluzioni del Consiglio di sicurezza delle Nazioni Unite (nota a CGCE 3 settembre 2008, cause riunite C-402/05 e C-415/05)*, in www.federalismi.it, 31 settembre 2008 ss.; B. Conforti, *Decisioni del Consiglio di sicurezza e diritti fondamentali in una bizzarra sentenza del Tribunale comunitario di primo grado, in Il Dir. dell'Unione europea*, 2006, 1, 333; C. Tomuschat, *Primacy of the United Nations Law. Innovation Features in the Community Legal Order*, in *Common Market Law Review*, 2006, 537; V. Sciarabba, *I diritti e i principi fondamentali nazionali ed europei e la problematica comunitarizzazione delle risoluzioni antiterrorismo dell'ONU, in Rivista AIC*, 23 dicembre 2005.

È un riappropriarsi di una sovranità, in fondo mai messa in discussione né ceduta, sul terreno ultimo dei diritti fondamentali, proprio quel terreno che l'Unione europea aveva conosciuto soltanto di riflesso nella sua prima stagione, scontando la vocazione prettamente mercantilistica della costruzione comunitaria. I diritti fondamentali, prima relegati –come già ricordato- a mere eccezioni in grado di giustificare, da parte degli Stati membri, restrizioni alle libertà economiche proclamate dai Trattati, divengono così perno del sistema e 'valvola' che ne regola l'apertura verso l'esterno.

Non può quindi passare inosservato e, al contrario, non definirsi centrale il ruolo della Carta dei diritti fondamentali dell'Unione europea, già cruciale in *Kadi.*

Proprio richiamando questa saga, però, si deve evidenziare una differenza di grande momento che sembra poter marcare ancora di più l'autonomia dell'ordinamento comunitario.

Nella vicenda *Kadi,* infatti, la fonte 'esterna' da cui era derivato un pregiudizio per i diritti fondamentali tutelati dalla Carta era rappresentata dagli obblighi imposti da un accordo internazionale, e più precisamente da una risoluzione del Consiglio di sicurezza delle Nazioni Unite. Era dunque nei confronti dell'ordinamento delle Nazioni Unite che il sistema comunitario doveva prendere le distanze, interponendo la tutela dei diritti fondamentali come ostacolo a una piena e pedissequa attuazione di quanto previsto dalla fonte eteronoma sulla quale il regolamento del Consiglio poi oggetto di (parziale) annullamento si appoggiava.

Nel caso *Schrems,* invece, non è una norma di diritto internazionale o un atto proveniente da un'organizzazione internazionale ma sono piuttosto il sistema di *Safe Harbor* e, in definitiva, l'ordinamento degli Stati Uniti a condurre l'Unione europea a esporre a minaccia i diritti fondamentali. Quindi, è nei confronti dell'ordinamento di uno stato terzo che si aziona il 'controlimite' che impone di munire di tutela gli artt. 7, 8 e 47 della Carta. Qui si apprezza a maggior ragione il valore della Carta, poiché il suo *enforcement* conduce a una rivisitazione, chiaramente *fundamental rights oriented*, di un atto racchiudeva una diversa valutazione del livello di tutela offerto dall'ordinamento statunitense: non la sostanziale riproduzione del contenuto di una norma di diritto internazionale, ma una valutazione, consolidata nella decisione 2000/250, di adeguatezza della tutela (e quindi di 'non pericolo' per i diritti fondamentali) viene riformata.

Sempre nel tentativo di allacciare la pronuncia *Schrems* con la narrativa europea in tema di diritti fondamentali, non si può non cogliere un collegamento importante tra un passaggio della sentenza e alcuni importanti

precedenti della Corte costituzionale tedesca.

Al punto 73, infatti, si legge che non si può esigere «che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione». Questa affermazione della Corte di Lussemburgo rievoca il significato di due rilevantissime sentenze del Tribunale federale costituzionale tedesco (*Bundesverfassungsgericht*), conosciute sotto il nome di *Solange I*[70] e *Solange II*[71].

La sentenza *Solange I*[72]*,* che risale al 1974, verte sull'interpretazione della clausola attributiva della sovranità a organizzazioni internazionali, racchiusa nell'art. 24. Secondo il *Bundesverfassungsgericht,* alla luce dello stadio ancora parziale dell'integrazione europea -testimoniato dall'assenza di un documento che tutelasse i diritti fondamentali e da un più generale problema di *deficit* democratico della costruzione comunitaria, il diritto comunitario avrebbe dovuto formare oggetto di un'interpretazione restrittiva. Di conseguenza, nell'assenza di un catalogo dei diritti fondamentali, il Tribunale costituzionale si riservava il diritto di non applicare le disposizioni del diritto comunitario contrarie ai diritti protetti dalla Costituzione tedesca.

Questa impostazione è stata rivisitata nella successiva pronuncia *Solange II,* del 1986, in cui il Tribunale di Karlshrue prendeva atto della capacità della Corte di giustizia di offrire –ed ecco qui la ridondanza con il punto 73 della sentenza *Schrems*[73]- un livello di tutela dei diritti fondamentali sostanzialmente paragonabile a quello della Legge fondamentale tedesca, in grado di preservarne il contenuto essenziale. In questo modo, il Tribunale costituzionale federale dichiarava che, fintantoché tali condizioni fossero perdurate, non avrebbe esercitato la propria giurisdizione (pur non spogliandosi formalmente di tale potere) per sindacare l'applicabilità del diritto comunitario derivato secondo il parametro dei diritti fondamentali sanciti dalla Costituzione. Il progresso nel percorso di integrazione europea verificatosi nel corso dei dodici anni che separano le due pronunce, evidentemente, deve aver convinto il giudice delle leggi tedesco sulla capacità di tenuta dell'ordinamento comunitario nel garantire il con-

[70] *BVerfGE* 37, 271.

[71] *BVerfGE* 73, 339.

[72] Per alcuni commenti, si v. S. Mangiameli, *L'esperienza costituzionale europea,* Roma, 2008, 30; P. Costanzo-L. Mezzetti-A. Ruggeri, *Lineamenti di diritto costituzionale dell'Unione europea*, Torino 2014; P.L. Geti, *Il contributo della Giurisprudenza costituzionale tedesca nella determinazione dei rapporti con l'Unione Europea,* relazione al convegno «Parlamenti nazionali e Unione europea nella governance multilivello», Roma, 12-13 maggio 2015.

[73] Cfr. F.C. Mayer, *The Force awakens – The Schrems case from a German perspective*, in www.verfassungsblog.de, 19 ottobre 2015.

tenuto essenziale dei diritti fondamentali, rispetto ai quali si è formata, nel diritto dell'Unione, una sensibilità crescente, come già rilevato.

Restando in tema di equivalenza del livello di protezione, infine, non si può non menzionare un terzo caso che rappresenta la dinamica tra corti costituzionali ed europee nella ricerca di un equilibrio di sistema. Nella sentenza *Bosphorus c. Irlanda* del 30 giugno 2005[74], la Corte europea dei diritti dell'uomo si è pronunciata in maniera storica sul tema della sindacabilità in base alla CEDU delle norme di diritto derivato dell'Unione, e segnatamente norme contenute in regolamenti[75].

È alla sentenza *Bosphorus* che risale l'enunciazione della *presumption of conventionality*. Invero, la Corte di Strasburgo aveva già affermato, nella sua giurisprudenza, l'insussistenza di una responsabilità per gli Stati membri dell'Unione europea per violazione della CEDU quando la loro condotta fosse originata dall'osservanza di norme di diritto derivato sulle quali (come nel caso dei regolamenti, direttamente applicabili) gli Stati non dispongono di alcun potere discrezionale, a condizione che nel sistema comunitario i diritti fondamentali ricevessero una protezione equivalente a quella prevista dalla CEDU.

Nella sentenza *Bosphorus* la Corte rifinisce questo principio, precisando come il principio di equivalenza debba intendersi in un'ottica di comparabilità tra i sistemi. Così al punto 155: «By 'equivalent' the Court means 'comparable'; any requirement that the organisation's protection be 'identical' could run counter to the interest of international cooperation pursued […]. However, any such finding of equivalence could not be final and would be susceptible to review in the light of any relevant change in fundamental rights protection».

Dunque le autorità degli Stati membri non possono rispondere di violazioni delle Convenzione, se agiscono in ossequio a norme direttamente applicabili dell'Unione europea. Tale presunzione, per cui gli Stati membri assicurano una protezione equivalente, può essere smentita solo nel caso in cui la tutela dei diritti fissati dalla CEDU sia manifestamente insufficiente.

Sul punto, basti ricordare che quella che é apparsa come la possibile chiusura del sistema, ossia l'adesione alla CEDU dell'Unione europea –allo stato soltanto annunciata, e giudicata incompatibile con lo stato

[74] Corte europea dei diritti dell'uomo, 30 giugno 2005, *Bosphorus Hava Jollari Turizm ve Ticaret*, n. 45036/98.

[75] Si vv., tra gli altri, i commenti di G. Repetto, *La Corte di Strasburgo e il sindacato sugli atti comunitari: al solange non c'è mai fine?*, in *Rivista AIC,* 2005; E. Cannizzaro, *Sulla responsabilità internazionale per condotte di Stati membri dell'Unione europea: in margine al caso Bosphorus*, in *Riv. dir. internaz.,* 2005, 3, 762 ss.

degli atti dalla Corte di giustizia in un recente parere[76], sembra un disegno ancora lontano dal potersi concretizzare[77]. Rimane così aperto, e la casistica ne conferma l'attualità, il tema della effettiva equivalenza (*rectius*: comparabilità) tra le garanzie stabilite a livello dell'Unione europea e della CEDU a tutela dei diritti fondamentali[78].

All'esito di questo percorso, si devono articolare due importanti rilievi conclusivi.

Dapprima, è interessante notare come, comparando la sentenza *Schrems* con la narrativa europea in tema di equivalenza della protezione dei diritti fondamentali, balzi immediatamente all'attenzione del costituzionalista la peculiarità di questo caso. Mentre, infatti, nei tre casi ricordati, il tema dell'equivalenza veniva in rilievo nel rapporto tra la Corte di giustizia e un ordinamento nazionale (nei casi *Solange I* e *II),* ovvero tra la Corte di giustizia e un ordinamento globale (nella saga *Kadi*), ovvero ancora tra Corte europea dei diritto dell'uomo e un ordinamento regionale (nel caso *Bosphorus*), così non è nella fattispecie in esame. Laddove, invece, la Corte di giustizia si pronuncia sul rapporto di equivalenza che collega l'ordinamento comunitario a quello statunitense: per la prima volta, il protagonista è uno stato, non un ordinamento internazionale, regionale o globale che sia. Questo singolare aspetto non appare immune dal generare possibili criticità, ponendo mente non solo al rischio di isolamento di cui si è detto, che potrebbe ingenerarsi

[76] Corte di giustizia dell'Unione europea, 18 dicembre 2014, parere n. 2/13. Per alcuni commenti, si v. F. Cherubini, *In merito al parere 2/13 della Corte di giustizia dell'UE: qualche considerazione critica e uno sguardo* de jure condendo, in *Osservatorio costituzionale,* maggio 2015; I. Anrò, *Il parere 2/13 della Corte di giustizia sul progetto di accordo di adesione dell'Unione europea alla CEDU: una bocciatura senza appello?,* in www.eurojus.it, 22 dicembre 2014; S. Peers, *The CJEU and the EU's accession to the ECHR: a clear and present danger to human rights protection*, in www.eulawanalysis.blogspot.it, 18 dicembre 2014; L. Besselink, *Acceding to the ECHR notwithstanding the Court of Justice Opinion 2/13,* in www.verfassungsblog.de, 23 dicembre 2014; S. Douglas-Scott, *Opinion 2/13 on EU accession to the ECHR: a Christmas bombshell from the European Court of Justice,* in www.ukconstituionallaw.org. 24 dicembre 2014..

[77] Sui problemi di coordinamento tra i sistemi, v. E. Gianfrancesco, *Incroci pericolosi: CEDU, Carta dei diritti fondamentali e Costituzione italiana tra Corte costituzionale, Corte di Giustizia e Corte di Strasburgo*, in *Rivista AIC*, 2011, 1.

[78] Cfr. in proposito V. Zagrebelsky, *L'UE e il controllo esterno della protezione dei diritti e delle libertà fondamentali in Europa. La barriera elevata dalla Corte di Giustizia,* in *DUDI,* 2015, 1 ss.; S. Douglas-Scott, *The Relationship between the EU and the ECHR Five Years on from the Treaty of Lisbon*, in S. de Vries-U. Bernitz-S. Weatherill (eds.), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old and Growing*, Oxford, 2015; O. De Schutter, Bosphorus *Post-Accession: Redefining the Relationships between the European Court of Human Rights and the Parties,* in V. Kosta-N. Skoutaris-V. Tzevelekos (eds.), *The EU Accession to the ECHR*, Oxford, 2014, 177 ss.

come conseguenza di un effetto domino legato al reciproco intersecarsi di valutazioni che dipendono dalla constatazione formulata in origine dalla Commissione, e ora smentita dalla Corte di giustizia; ma anche ai profili di carattere 'diplomatico' e di «comity» che riguarderanno i rapporti tra gli Stati Uniti e l'Unione europea nei mesi a venire. Un crinale, questo, già caldo alla luce della recentissima approvazione del nuovo regolamento in materia di protezione dei dati personale, che esaurite le ultime battute entrerà a breve in vigore[79].

Il secondo rilievo è connesso al ruolo degli attori coinvolti nella vicenda. Negli altri casi in cui si è espressa, la Corte di giustizia disponeva degli strumenti non solo per affermare un principio ma anche per garantirne in concreto l'attuazione: il soggetto competente a valutare il canone di equivalenza era in altri termini lo stesso che aveva enunciato e costruito quel principio e quella clausola. Così non è, invece, nel caso *Schrems,* dove per un verso la Corte di giustizia demolisce l'impianto della decisione adottata dalla Commissione con cui era stata constatata l'adeguatezza del sistema di *Safe Harbor* statunitense. Ma, dopo aver manipolato e ricostruito in termini differenti il parametro rilevante, muovendo dall'adeguatezza alla sostanziale equivalenza, di fatto la Corte affida alle autorità nazionali il compito di condurre questo apprezzamento, avviando un importante moto di decentralizzazione: ciò che prima era definito a livello comunitario, ora trova sistemazione a livello dei singoli Stati membri.

Questo approccio, tuttavia, sembra iscriversi in una direzione opposta a quella auspicata, per esempio dal'Article 29 Working Party, che in uno *statement*[80] reso a ridosso della sentenza ha ribadito l'esigenza di una «*robust, collective and common position on the implementation of the judgment*». Al contrario, sembra che nell'approccio della Corte possa prevalere un processo di decentralizzazione e disomogeneizzazione di ciò che precedentemente era definito a livello europeo: una porta aperta verso una balcanizzazione della tutela[81], affidata alla sensibilità delle autorità nazionali e, così, sempre più a macchia di leopardo. Un rischio che sarebbe meglio evitare.

[79] Commissione europea, Protezione dei dati nell'UE: l'accordo sulla riforma proposta dalla Commissione stimolerà il mercato unico digitale, Bruxelles, 15 dicembre 2015.

[80] Article 29 Working Party Statement on the implementation of the Court of Justice of the European Union of 6 October 2015, cit.

[81] E. Morozov, *The World Is Not Enough – How To Reinvent The Internet,* in *Sueddeutsche Zeitung*, 20 gennaio 2014. Si v. anche S. Alves Jr., *Internet Governance 2.0.1.4: The internet balkanization fragmentation,* 20th ITS Biennial Conference, «The Net and the Internet - Emerging Markets and Policies», Rio de Janeiro, 2014. Sia consentito altresì rinviare a O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo?,* cit., 26-27.

Abstract

The reasoning of the Court of Justice in the Schrems judgment places this decision in the wake of the judicial saga commenced with the Digital Rights Ireland and Google Spain cases. Also in this decision, in fact, the Court of Luxembourg has taken it seriously the right to privacy, in light of the threats and risks arising from the broader and broader circulation of personal data, especially through the Internet. When invalidating the decision of the Commission concerning the adequacy of the Safe Harbour Principles, the Court of Justice has once again enforced in a very extensive manner the Charter of Fundamental Rights of the European Union, and particularly Articles 7 and 8. This has led the Court, indeed, to convert the adequacy standard for personal data to be transferred to non-EU countries in the requirement of equivalent protection. This decision, however, this decision is likely to bring unprecedented consequences and global effects which cannot be limited to the European Union territory.

Giusella Finocchiaro

La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain *a* Schrems

Sommario: Introduzione. – 1. Le scelte politiche. – 2. Gli argomenti giuridici. – 2.1. La rilevanza degli artt. 7 e 8 della Carta dei diritti fondamentali. 2.2. L'interpretazione estensiva della nozione di 'stabilimento'. – 3. Ulteriori indicazioni interpretative. – 3.1. La pluralità di leggi nazionali applicabili. – 3.2. Distinzione fra 'dato personale' e 'valutazione'. Definizione di 'trattamento'. – 3.3. Bilanciamento fra il diritto all'accesso ai documenti amministrativi e il diritto alla protezione dei dati personali. – 3.4. Trattamento dei dati personali da parte di un'autorità amministrativa. Obbligo di informativa. – 3.5. Elementi biometrici dei passaporti e dei documenti di viaggio. – Conclusioni

Introduzione

La giurisprudenza della Corte di giustizia europea in materia di dati personali da *Google Spain* a *Schrems* appare piuttosto ricca, a conferma della rilevanza strategica che ha assunto questo tema nell'Unione europea.

Si tratta di una decina di sentenze in meno due anni, elencate in nota[1],

[1*]Il commento rientra nell'ambito del PRIN 2010 - 2011, «La regolamentazione giuridica delle Tecnologie dell'Informazione e della Comunicazione (TIC) quale strumento di potenziamento delle società inclusive, innovative e sicure». Le sentenze della Corte di giustizia europea riguardanti il trattamento di dati personali, che succedono alla sentenza del 13 maggio 2014, *Google Spain, Google Inc. e Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* (causa C-131/12) sono elencate di seguito: Corte di giustizia, sentenza del 17 luglio 2014, cause riunite C-141/12 e C-372/12, *Y.S. e a.*; Corte di giustizia, sentenza del 2 ottobre 2014, causa C-127/13 P, *Strack/Commissione*; Corte di giustizia, sentenza dell'11 dicembre 2014, causa C-212/13, *Ryneš*; Corte di giustizia, sentenza del 16 aprile 2015, cause riunite da C-446/12 a C-449/12, *Willelms e a.*; Corte di giustizia, sentenza del 16 luglio 2015, causa C-615/13 P, *ClientEarth e PAN Europe/EFSA*; Corte di giustizia, sentenza del 16 luglio 2015, causa C-580/13, *Coty Germany;* Corte di giustizia, sentenza del 1° ottobre 2015, causa C-201/14, *Bara e a.*; Corte di giustizia, sentenza del 1° ottobre 2015, causa C-230/14, *Weltimmo*; Corte di giustizia, sentenza del 6 ottobre 2015, causa C-362/14, *Schrems,* cui si aggiunge per rilevanza, come sopra anticipato, Corte di giustizia, sentenza dell'8 aprile 2014, cause

cui si aggiunge per importanza, pur essendo di poco antecedente alla decisione *Google Spain*, la sentenza dell'8 aprile 2014, *Digital Rights Ireland* e *Seitlinger e a.* (cause riunite C-293/12 e C-594/12) [2].

riunite C-293/12 e C-594/12*, Digital Rights Ireland* e *Seitlinger e a.* Le sentenze possono essere tutte reperite all'URL www.curia.europa.eu .

[2] Si fa riferimento alla decisione della Corte di giustizia dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e a*. La sentenza ha origine da due distinte domande di pronuncia pregiudiziali riunite, presentate rispettivamente dalla High Court (Irlanda) e dal Verfassungsgerichtshof (Austria). Le domande di pronuncia pregiudiziale vertono sulla validità della direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, che modifica la direttiva 2002/58/CE. La Corte di giustizia dichiara la direttiva 2006/24/CE invalida, rilevando che: data l'estrema diffusione dei mezzi di comunicazione elettronica, la direttiva ha ingerenza sui diritti fondamentali della quasi totalità della popolazione europea; la direttiva riguarda in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi; la direttiva non prevede alcun criterio oggettivo né le condizioni sostanziali o procedurali che permettano di delimitare l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore; la direttiva impone un periodo di conservazione dei dati di sei mesi ma non effettua alcuna distinzione tra le categorie di dati a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate e non determina la durata di conservazione in base a criteri obiettivi al fine di garantire che sia limitata allo stretto necessario. La Corte rileva, infine, che dal momento che tale direttiva non impone che i dati siano conservati sul territorio dell'Unione, non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, comma 3, della Carta dei diritti fondamentali dell'Unione europea. Conseguentemente la Corte ritiene che il legislatore dell'Unione abbia ecceduto i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, comma 1, della Carta dei diritti fondamentali dell'Unione europea. In particolare sostiene che la direttiva non sia frutto di un corretto bilanciamento tra la necessità di garantire la sicurezza pubblica contro la criminalità grave, attraverso la conservazione dei dati personali nell'ambito delle comunicazioni elettroniche, e il diritto dei cittadini alla protezione dei dati personali, sotto il profilo del diritto fondamentale al rispetto della vita privata.

1. Le scelte politiche

Si leggono alcune tendenze, evidenti nelle due decisioni più note, *Google Spain* e *Schrems* [3], ma presenti anche in altre, di carattere politico[4], anticipatorie rispetto alle scelte ormai quasi compiute nell'emanando regolamento[5].

[3] A differenza di quanto verrà effettuato per le altre decisioni non si ritiene opportuno riassumere il contenuto delle due decisioni, rispettivamente oggetto di un numero monografico di *Dir. Inf.* il n. 4/5 del 2014, nonché di questo *Dir. Inf.* olume. Ci si limita qui a ricordare che i principi di diritto affermati nella decisione *Google Spain* sono tre. In primo luogo, la sentenza afferma che si applica la legge nazionale del Paese nel quale il motore di ricerca opera, esercitando anche altre attività, quali la promozione e la vendita degli spazi pubblicitari. In secondo luogo, che Google, e in generale i motori di ricerca, sono «titolari del trattamento» e pertanto che l'interessato ha il diritto di richiedere che sia rimossa l'indicizzazione direttamente al motore di ricerca, a prescindere da ogni richiesta al gestore del sito *web* che ha pubblicato l'informazione, anche nel caso in cui l'informazione sia stata e sia legittimamente pubblicata sul sito *web*. In terzo luogo, che l'interessato «ha diritto a che l'informazione riguardante la sua persona non venga più collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome» e che «nel valutare i presupposti di applicazione di tali disposizioni, si deve verificare in particolare se l'interessato abbia diritto a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome, senza per questo che la constatazione di un diritto siffatto presupponga che l'inclusione dell'informazione in questione in tale elenco arrechi un pregiudizio a detto interessato». La recente decisione Schrems della Corte di giustizia europea invalida la decisione della Commissione nota come *Safe Harbour* e afferma che spetta agli Stati nazionali valutare se gli Stati Uniti siano da considerarsi un Paese che, ai sensi della direttiva-madre in materia di protezione dei dati personali, garantisce un livello di tutela adeguato.

[4] Evidenziano l'indirizzo politico assunto dalla Corte di giustizia già dal caso *Google*: Pollicino, *Un* digital right to *privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di* Google Spain, in *Dir. Inf.* 2014, p. 569 ss.; G. Sartor - M. Viola de Azevedo Cunha, *Il caso* Google *e i rapporti regolatori Usa/EU*, in *Dir. Inf.* 2014, p. 657 ss. e A. Mantelero, *Il futuro regolamento EU sui dati personali e la valenza 'politica' del caso* Google*: ricordare e dimenticare nella* digital economy, in *Dir. Inf.* 2014, p. 681 ss. La scelta della Corte di anticipare il contenuto dell'emanando regolamento è sottolineata da: P. Piroddi, *Questioni internazionalprivatistiche sui motori di ricerca*, in *Dir. Inf.* 2014, p. 623 ss. e ancora da O. Pollicino, *op. cit.,* in particolare p. 587 ss., A. Mantelero, *op.cit.*

[5] Si tratta ovviamente della proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), adottata dalla Commissione il 25 gennaio 2012, n. 2012/0011 consultabile all'URL http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52012PC0011.Il 12 marzo 2014 anche il Parlamento europeo ha votato in prima lettura sulla proposta.

In estrema sintesi, la Corte vuole affermare l'applicabilità della normativa europea anche nel caso in cui i titolari di trattamento dei dati personali siano soggetti non europei e i dati vengano trattati prevalentemente fuori dall'Europa. Ribadisce il rango costituzionale del diritto alla protezione dei dati personali secondo la Carta dei diritti fondamentali dell'Unione europea e soprattutto la prevalenza di tale diritto sugli altri diritti, pure costituzionalmente garantiti, affermando così una scelta culturale e di principi[6]. Riafferma il carattere di eccezionalità delle limitazioni al diritto alla protezione dei dati personali. Assume che il livello di protezione dei dati personali adottato in Europa sia più elevato rispetto al livello di protezione dei dati personali adottato altrove nel mondo e si fa promotrice del modello europeo del diritto alla protezione dei dati personali. La Corte europea si riappropria e consolida la posizione volta ad affermare l'applicazione del diritto europeo al trattamento dei dati personali degli europei. Si tratta di indirizzi profondamente politici in cui la Corte orgogliosamente sceglie cultura, principi e diritto europeo, contrapponendosi alla visione e agli interessi, nei casi in esame, statunitensi[7].

La Corte esercita dunque un ruolo di supplenza politica, estendendo l'applicabilità della normativa europea e anticipando nell'interpretazione

Il 15 giugno 2015, dopo un lungo e travagliato iter di approvazione, anche il Consiglio «Giustizia e affari interni» ha raggiunto un accordo generale sulla proposta di regolamento, permettendo così l'apertura dei triloghi con il Parlamento europeo e la Commissione il 24 giugno 2015. A distanza di pochi mesi, in una riunione straordinaria tenutasi il 17 dicembre 2015, la Commissione per le libertà civili, la giustizia e gli affari interni del Parlamento europeo ha espresso la sua posizione sui testi concordati nei negoziati in forma di trilogo tra il Consiglio, il Parlamento europeo e la Commissione. Il 18 dicembre 2015 il Comitato dei rappresentanti permanenti (Coreper) ha approvato il testo di compromesso. I testi saranno ora presentati, ai fini dell'adozione di un accordo politico, in una prossima sessione del Consiglio. Dopo l'adozione della posizione del Consiglio in prima lettura, i testi saranno trasmessi al Parlamento per l'approvazione. Si prevede che il regolamento e la direttiva entreranno in vigore nella primavera del 2016 e saranno applicabili a partire dalla primavera del 2018. L'evoluzione dell'iter di approvazione del «pacchetto protezione dati» è consultabile nei seguenti siti, dai quali sono state tratte le informazioni sopra riassunte: http://eur-lex.europa.eu/legal-content/IT/HIS/?uri=CELEX:52012PC0011 - http://www.consilium.europa.eu/it/policies/data-protection-reform/ - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4443361

[6] Su questo punto, v. O. Pollicino, *op. cit.* che fra l'altro sottolinea il 'capovolgimento temporale' (*sic* p. 576) operato dalla Corte, secondo la quale sono gli artt. 7 e 8 della Carta a ricevere attuazione da parte di disposizioni di diritto derivato di cinque anni precedenti.

[7] Sul punto, v. G. Sartor - M. Viola de Azevedo Cunha, *op. cit.*, con ampia bibliografia.

della direttiva-madre l'emanando regolamento europeo sulla protezione dei dati personali.

Il fenomeno appare immediatamente leggibile nelle decisioni *Google Spain* e *Schrems* ma gli argomenti giuridici sono altresì ampiamente elaborati in *Digital Rights Ireland* e in *Weltimmo*[8].

2. Gli argomenti giuridici

I macroargomenti giuridici elaborati dalla Corte sono due. Innanzitutto la rilevanza degli artt. 7 e 8 della Carta dei diritti fondamentali e la prevalenza del diritto alla protezione dei dati personali e alla vita privata (prevalentemente intesi come un'endiadi) sugli altri diritti. In secondo luogo, l'interpretazione estensiva dell'art. 4 della direttiva sull'applicabilità territoriale della stessa e, in particolare, della nozione di 'stabilimento'.

2.1 La rilevanza degli artt. 7 e 8 della Carta dei diritti fondamentali

La Corte conferma ed enfatizza non solo la rilevanza costituzionale, ma anche la supremazia valoriale degli artt. 7 e 8 della Carta dei diritti

[8] La domanda di pronuncia pregiudiziale verte sull'interpretazione degli articoli 4, paragrafo 1, lettera a), e 28, paragrafi 1, 3 e 6, della direttiva 95/46/CE. Nel caso di specie la Weltimmo, società registrata in Slovacchia, gestiva un sito Internet di annunci immobiliari riguardanti beni situati in Ungheria. Nell'ambito di tale attività, essa trattava i dati personali degli inserzionisti. A seguito di un'ipotesi di trattamento illecito dei dati, gli inserzionisti presentavano reclamo all'autorità ungherese preposta alla tutela dei dati personali, che comminava alla Weltimmo un'ammenda per aver violato la legge ungherese di attuazione della direttiva 95/46/CE. La Weltimmo contestava la decisione dell'autorità di controllo ungherese adducendo che non avrebbe potuto irrogare l'ammenda non avendo titolo per applicare la legge del proprio paese, adottata sulla base della direttiva 95/46/CE. Chiamata a dirimere la controversia, la Corte suprema adiva la Corte di giustizia per chiarire se, nel caso di specie, la direttiva consentisse all'autorità ungherese di controllo di applicare la legge ungherese adottata sulla base della direttiva e di imporre l'ammenda prevista da tale legge. Secondo la Corte di giustizia, come si avrà modo di illustrare nel corso di questo lavoro, l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46/CE, deve essere interpretato nel senso che esso consente l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si svolge tale trattamento.

fondamentali dell'Unione europea[9] che si riferiscono rispettivamente al rispetto della vita privata e della vita familiare e alla protezione dei dati di carattere personale e che costituiscono, come la Corte ribadisce, la base per l'interpretazione della direttiva 95/46/CE[10].

Come è noto, l'art. 8 della Carta, significativamente fra i diritti di libertà, afferma il diritto alla protezione dei dati personali, e precisamente che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Afferma, inoltre, che i dati personali devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge e che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Sempre nell'art. 8 si afferma che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente[11].

Tale diritto è distinto dal diritto alla protezione della vita privata, altra formulazione del diritto alla riservatezza, riconosciuto dall'art. 7 della Carta, ove si afferma il diritto al rispetto della vita privata e della vita familiare: ogni individuo, dispone la norma, ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.

Il diritto alla protezione dei dati personali ha un oggetto estremamente vasto, che è conseguenza della stessa definizione di dato personale. Muovendo, infatti, dall'ampia definizione di dato personale, il diritto alla protezione dei dati personali si configura come il diritto di un soggetto di controllare l'insieme delle informazioni che al medesimo si riferiscono e che quindi costituiscono il suo riflesso e delineano lo stesso suo essere nella società dell'informazione.

Il diritto alla protezione dei dati personali è anche noto come «information privacy», «informational privacy», «data privacy», tutte espressioni nelle quali si evidenzia che l'oggetto del diritto è l'informazione o il dato, benché a rigore dato e informazione siano termini non coincidenti.

Il diritto alla protezione dei dati personali deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni. Per questa ragione è frequente che il diritto alla protezione dei dati

[9] In tal senso, *ex multis, Digital Rights Ireland*, punto 53; *Google Spain*, punti 53, 66 e 74 nonché Schrems, punto 39.
[10] Così *Google Spain* punto 68; *Ryneš*, punto 29 e *Schrems*, punto 38.
[11] Per approfondimenti si rinvia a G. Finocchiaro, *Privacy e protezione dei dati personali*, Zanichelli, Bologna, 2012.

personali sia inteso come diritto all'autodeterminazione informativa, cioè alla scelta di ogni soggetto di autodefinirsi e determinarsi.

Il necessario carattere di eccezionalità delle deroghe al diritto fondamentale alla tutela dei dati personali è sancito nella decisione *Digital Rights Ireland* ove si afferma che la direttiva 2006/24/CE (annullata dalla medesima decisione) non prevedendo «norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta, comporta un'ingerenza nei suddetti diritti fondamentali di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario»[12]. Nella stessa decisione si afferma inoltre il ruolo essenziale dell'autorità di controllo da parte di un'autorità indipendente che «costituisce un elemento essenziale del rispetto della tutela delle persone riguardo al trattamento dei dati personali (v., in tal senso, sentenza Commissione/Austria, C-614/10, EU:C:2012:631, punto 37)»[13].

L'obiettivo della protezione dei dati personali dei cittadini europei che comporta un'estensione dell'ambito di applicazione della direttiva conduce addirittura a formulare l'ulteriore requisito che i dati siano conservati nel territorio europeo. Questa materializzazione della protezione è formulata nella sentenza *Digital Rights Ireland*, ove si afferma che dal momento che la direttiva 2006/24/CE (come si è detto, annullata nella medesima decisione) non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione, non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3, della Carta dei diritti fondamentali [14].

I medesimi argomenti sono più ampiamente sviluppati nel caso *Schrems* ove si afferma che una normativa europea «che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l'applicazione della misura *de qua* e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati».

E nella stessa decisione, riferendosi evidentemente al trattamento

[12] Punto 65 della decisione *Digital Rights Ireland*.
[13] Punto 68 della decisione *Digital Rights Ireland*.
[14] Così il punto 68 della sentenza *Digital Rights Ireland*. V. in senso critico O. Pollicino, *op. cit.*, in particolare p. 587.

attraverso i *social network*, si precisa altresì che tali garanzie acquisiscono maggiore importanza «allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (sentenza Digital Rights Ireland e a., C293/12 e C594/12, EU:C:2014:238, punti 54 e 55, nonché la giurisprudenza ivi citata)» [15].

Nella medesima decisione si richiama il principio che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario [16]. Ciò conduce la Corte a ritenere che non sia conforme al citato principio una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta e che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta [17].

La Corte sottolinea la necessità della previsione per il singolo di potersi avvalere di rimedi giuridici per esercitare il proprio diritto al controllo sui suoi dati personali, controllo che costituisce l'essenza del diritto stesso alla protezione dei dati personali, e ribadisce che «l'esigenza di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto (v., in tal senso, sentenze Les Verts/Parlamento, 294/83, EU:C:1986:166, punto 23; Johnston, 222/84, EU:C:1986:206, punti 18 e 19; Heylens e a., 222/86, EU:C:1987:442, punto 14, nonché, UGTRioja e a., da C428/06 a C434/06, EU:C:2008:488, punto 80)»[18] .

L'eccezionalità delle deroghe al diritto alla protezione dei dati personali è richiamata anche dalla sentenza dell'11 dicembre 2014, causa C-212/13, *Ryneš*[19]. In questa decisione la Corte ribadisce l'eccezionalità dell'esclu-

[15] Così il punto 91 della sentenza *Schrems*.
[16] Così il punto 92 della sentenza *Schrems*.
[17] Così i punti 93 e 94 della sentenza *Schrems*.
[18] Così il punto 95 della sentenza *Schrems*.
[19] Nel caso di specie viene contestato al sig. Ryneš un illecito trattamento dei dati personali avvenuto attraverso l'installazione di un sistema di videosorveglianza all'esterno dell'abitazione personale, senza informare e richiedere il consenso dei passanti 'videore-

sione prevista dall'art. 3 della direttiva per il trattamento effettuato per ragioni personali o familiari [20].

2.2 L'interpretazione estensiva della nozione di 'stabilimento'

Nelle decisioni in esame la Corte estende l'ambito di applicazione della direttiva. In particolare, l'*iter* argomentativo utilizzato muove dall'interpretazione estensiva dell'art. 4 e della nozione di 'stabilimento', che conduce ad anticipare l'applicazione dell'art. 3 dell'emanando regolamento [21].

Infatti, secondo l'art. 4, comma 1, della direttiva, «Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:

a) effettuato nel contesto delle attività di uno stabilimento del responsabile[22] del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati

gistrati'. Il sig. Ryneš adduceva che il sistema di videosorveglianza era stato installato per tutelare la vita sua e dei propri familiari, in quanto diritto fondamentale e inviolabile, e che il trattamento dei dati in questione rientrava nell'«esercizio di attività a carattere esclusivamente personale o domestico», escludendo l'applicabilità della direttiva 95/46/CE e dei conseguenti obblighi informativi e di raccolta del consenso per il trattamento.

[20] Così *Ryneš*, punto 28.

[21] Sulla nozione di stabilimento v. G. Caggiano, *L'interpretazione del «contesto delle attività di stabilimento» dei responsabili del trattamento dei dati personali, in Dir. Inf.* 2014, p. 605 ss.

[22] Si ricorda che la definizione di 'responsabile' di trattamento fornita dalla direttiva all'art. 2, comma 1, lett. d) è la seguente: «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario". Essa dunque corrisponde alla definizione di 'titolare' del trattamento dei dati personali nel diritto italiano, che si legge all'art. 4, comma 1, lett. f) del decreto legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali, che definisce 'titolare', «la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza».Una figura analoga a quella del responsabile del trattamento prevista dal Codice in materia di protezione dei dati personali italiano non è invece contemplata dalla direttiva, la quale prevede due sole figure: il responsabile ('titolare' nell'attuazione italiana della direttiva) e l'incaricato (definito 'incaricato' anche nel Codice italiano).

membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile; […]» [23].

Cruciale diviene quindi l'interpretazione della nozione di 'stabilimento', che viene dilatata fino a divenire «nel contesto delle attività di uno stabilimento», contrapponendo così l'attività di trattamento 'nel contesto' e l'attività di trattamento 'in senso proprio', come si legge nelle conclusioni dell'avvocato generale nel caso *Weltimmo*. Ivi si legge altresì che l'articolo 4, paragrafo 1, lettera a), svolge una duplice funzione, consentendo da un lato, l'applicazione del diritto dell'Unione attraverso il diritto di uno dei suoi Stati membri quando il trattamento dei dati abbia luogo esclusivamente 'nel contesto' delle attività di uno stabilimento situato nel loro territorio, e ciò anche se il trattamento dei dati 'in senso proprio' viene effettuato in un terzo Stato (come accadeva nella causa *Google Spain* e *Google*) e consentendo dall'altro, di determinare la legge applicabile in quanto norma di conflitto tra le leggi dei diversi Stati membri (come appunto nel caso *Weltimmo*) [24].

Nel caso *Google Spain* è esplicito il tentativo della Corte di ampliare l'ambito di applicazione territoriale della direttiva 95/46/CE, attraverso un'interpretazione estensiva dell'art. 4, per assicurare ai dati di cittadini europei, trattati fuori dai confini dell'Unione, le medesime garanzie assicurate ai trattamenti dei dati effettuati all'interno dell'Unione. In particolare nell'individuare il luogo al quale collegare l'applicazione

[23] Sui criteri di applicabilità della direttiva 95/46/CE e sulla qualificazione dei medesimi sotto il profilo del diritto internazionale, molto è stato scritto. Si rinvia a C. Kuner, *European Data Protection Law-Corporate Compliance and Regulation*, 3rd ed., Oxford, 2007 e in particolare al capitolo terzo per un ampio e approfondito inquadramento del tema, a P. Piroddi, *op. cit.,* la quale evidenzia i vizi argomentativi della decisione *Google*, nonché a L. Moerel, *Back to basics: when does EU data protection law apply?* in *International Data Privacy Law,* 2011, Vol. 1, No. 2, pp. 92-110 e Id., *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?* in *International Data Privacy Law*, 2011, Vol. 1, No. 1, pp. 28-46. In particolare Moerel ricostruisce la storia dell'art. 4 della direttiva e il passaggio dal criterio del paese di origine, che l'A. ritiene essere quello più efficace, chiaramente originariamente formulato, a criteri che conducono ad una pluralità di leggi nazionali applicabili. Si v. anche L.Colonna, *Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?* in *International Data Privacy Law*, 2014, Vol. 4, No. 3, pp. 203-22, fortemente critica sull'attuale art. 4 della direttiva, del quale fornisce una chiara illustrazione, ricordando i tre differenti approcci cui è riconducibile l'art. 4, rispettivamente basati sulla territorialità, sugli effetti e sulla protezione dei cittadini europei.

[24] Conclusioni dell'avvocato Generale in *Weltimmo*, punto 23.

della direttiva, la Corte ritiene rilevante non tanto il luogo in cui il trattamento dei dati viene fisicamente effettuato, quanto il luogo in cui la società che opera il trattamento esercita la propria attività, basata sul trattamento. Nel caso di specie la Corte osserva che Google Spain (con sede legale a Madrid) costituisce una filiale di Google Inc. (con sede legale negli Stati Uniti) nel territorio spagnolo e, pertanto, uno 'stabilimento' ai sensi della direttiva.

La Corte respinge l'argomento secondo cui il trattamento di dati personali da parte di Google Search non viene effettuato nel contesto delle attività di tale stabilimento in Spagna. La Corte considera al riguardo che, quando i dati vengono trattati per le esigenze di un motore di ricerca gestito da un'impresa che, sebbene situata in uno Stato terzo, dispone di uno stabilimento in uno Stato membro, il trattamento viene effettuato «nel contesto delle attività» di tale stabilimento, qualora quest'ultimo sia destinato ad assicurare, nello Stato membro in questione, la promozione e la vendita degli spazi pubblicitari proposti sul motore di ricerca al fine di rendere redditizio il servizio offerto da quest'ultimo[25].

Sui criteri per determinare il diritto applicabile e l'autorità competente di cui all'articolo 4 della direttiva 95/46/CE, dunque la Corte ripropone l'orientamento evidenziato in *Google Spain* nella recente sentenza *Weltimmo.* Pur essendo diverso il contesto in cui si inseriscono le due sentenze (mentre in *Google Spain* si discuteva sull'applicabilità o meno della direttiva a trattamenti di dati avvenuti fuori dai confini europei, in *Weltimmo* la controversia ha ad oggetto la determinazione di quale tra due legislazioni di Stati membri sia applicabile, in base allo Stato in cui il trattamento è avvenuto), in entrambe è centrale l'interpretazione del concetto di 'stabilimento' e di 'contesto delle attività'. Anche in *Weltimmo*, come in *Google Spain*, la Corte sottolinea come «l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 non esige che il trattamento di dati personali in questione venga effettuato 'dallo' stesso stabilimento interessato, bensì soltanto che venga effettuato 'nel contesto delle attività' di quest'ultimo"[26] e quindi che consenta «l'applicazione della legge in materia di protezione dei dati personali di uno Stato membro diverso da quello nel quale il responsabile del trattamento di tali dati è registrato, purché il medesimo svolga, tramite un'organizzazione stabile nel territorio di tale Stato membro, un'attività effettiva e reale, anche minima, nel contesto della quale si

[25] P. Piroddi, op. cit., p. 647, evidenzia che la Corte inverte totalmente i termini della questione. È l'attività commerciale di vendita di pubblicità che è effettuata nel cotesto delle attività del motore di ricerca e non viceversa.
[26] Così il punto 52 della sentenza *Google Spain*.

svolge tale trattamento».

In *Weltimmo* la sentenza *Google Spain* è espressamente richiamata, affermandosi che «l'espressione 'nel contesto delle attività di uno stabilimento' non può ricevere un'interpretazione restrittiva» e che «il legislatore dell'Unione ha quindi previsto un ambito di applicazione territoriale della direttiva 95/46 particolarmente esteso, che ha inserito all'articolo 4 della stessa» [27].

Un espresso invito all'interpretazione flessibile della nozione di stabilimento è formulato dall'avvocato generale in *Weltimmo* [28] e ripreso dalla Corte che si pronuncia per «una concezione flessibile della nozione di stabilimento, che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata. Infatti, per determinare se una società, responsabile di un trattamento dei dati, dispone di uno stabilimento, ai sensi della direttiva 95/46, in uno Stato membro diverso dallo Stato membro o dal paese terzo in cui è registrata, occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione. Ciò vale soprattutto per imprese che offrono servizi esclusivamente tramite Internet.

A questo proposito, occorre segnatamente considerare, alla luce dell'obiettivo perseguito da tale direttiva, consistente nel garantire una tutela efficace e completa del diritto alla vita privata e nell'evitare che le disposizioni vengano eluse, che la presenza di un unico rappresentante, in talune circostanze, può essere sufficiente a costituire un'organizzazione stabile se il medesimo opera con un grado di stabilità sufficiente con l'ausilio dei mezzi necessari per la fornitura dei servizi concreti di cui trattasi nello Stato membro in questione.

[27] Così i punti 25 e 27 della sentenza *Weltimmo.*

[28] Così nel punto 28 delle conclusioni: «Ciò detto, occorre fare riferimento al considerando 19 della direttiva 95/46, che costituisce un elemento di interpretazione fondamentale per determinare il contenuto della nozione di stabilimento ai sensi della medesima direttiva. Detto considerando suggerisce una concezione flessibile della nozione in parola, che si discosta dall'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata. Infatti, in primo luogo, detto considerando comprende un criterio di effettività e un elemento di stabilità laddove enuncia che "lo stabilimento nel territorio di uno Stato membro implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile […]". In secondo luogo, esso offre una notevole flessibilità disponendo che 'la forma giuridica di siffatto stabilimento, si tratti di una semplice succursale o di una filiale dotata di personalità giuridica, non è il fattore determinante a questo riguardo».

Inoltre, per realizzare detto obiettivo, occorre considerare che la nozione di 'stabilimento', ai sensi della direttiva 95/46, si estende a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile» [29]. E l'avvocato generale giunge a sostenere che sia sufficiente «un operatore con una presenza duratura, dotato di poco più di un computer portatile» [30]. Richiama, quindi, le interpretazioni della nozione di stabilimento formulate in altri settori del diritto europeo[31] e sottolinea, come già nelle conclusioni dell'avvocato generale nel caso *Google*, la necessità di valutare la particolarità delle attività economiche esercitate tramite Internet[32]. Come argomenta l'avvocato generale, questa valutazione è stata già effettuata nella direttiva sul commercio elettronico ove si enuncia al considerando 19 che «[…] [i]l luogo di stabilimento, per le società che forniscono servizi tramite siti Internet, non è là dove si trova la tecnologia di supporto del sito né là dove esso è accessibile, bensì il luogo in cui tali società esercitano la loro attività economica» e tale definizione è stata ritenuta pertinente dal Gruppo articolo 29[33] al fine di interpretare l'articolo 4 della direttiva 95/46/CE[34].

In questo stesso senso, occorre ricordare, si esprime anche il *Model*

[29] Punti 29, 30 e 31 della sentenza Weltimmo.

[30] Punto 34 delle conclusioni dell'avvocato generale nella sentenza *Weltimmo*.

[31] Punto 29. Siffatta concezione della nozione di stabilimento è in linea con l'interpretazione che tale nozione ha ricevuto nella giurisprudenza della Corte in altri settori del diritto dell'Unione. In particolare, secondo costante giurisprudenza, «la nozione di stabilimento di cui alle disposizioni del Trattato relative alla libertà di stabilimento implica l'esercizio effettivo di un'attività economica per una durata di tempo indeterminata, mercé l'insediamento in pianta stabile in un altro Stato membro», il che «presuppone […] un insediamento effettivo della società interessata nello Stato membro ospite e l'esercizio quivi di un'attività economica reale». Punto 30. Inoltre, il parere n. 8/2010 del Gruppo articolo 29 fa riferimento all'interpretazione della nozione di stabilimento in quanto criterio di collegamento ai fini fiscali in materia di IVA. La giurisprudenza della Corte in tale materia risulta particolarmente interessante – giacché la nozione di stabilimento opera come criterio di collegamento per determinare l'assoggettamento a una normativa tributaria nazionale – e approfondisce la nozione di stabile organizzazione, che «[…] dev'essere caratterizzata da un sufficiente grado di permanenza e da una struttura adeguata, in termini di risorse umane e tecniche, che le consentano di ricevere ed utilizzare i servizi fornitile per le specifiche esigenze delle organizzazioni medesime». Inoltre, la nozione di stabilimento presente sia nell'ambito della Convenzione di Roma che in quello della Convenzione di Bruxelles milita parimenti a favore di una concezione non formalistica.

[32] Punto 34 delle conclusioni dell'avvocato generale nella sentenza Weltimmo.

[33] Gruppo art. 29, Parere n. 8/2010 sul diritto applicabile, adottato il 16 dicembre 2010, 0836-02/10/IT, WP 179.

[34] Punto 35 delle conclusioni dell'avvocato generale nella sentenza Weltimmo.

Law sul commercio elettronico dell'Uncitral[35].

La Corte ritiene, invece, inconferente la questione della cittadinanza delle persone interessate da tale trattamento, così come il luogo in cui sono stati caricati i dati, lo Stato membro al quale sono rivolti i servizi, la nazionalità degli interessati o il luogo in cui risiedono i titolari dell'impresa[36] .

In tal senso si pronuncia anche il Gruppo articolo 29, secondo cui «[n]on sono decisivi [al fine di determinare il diritto applicabile] la cittadinanza o il luogo di residenza abituale dell'interessato né l'ubicazione fisica dei dati personali»[37].

In *Google Spain* si evidenzia specificamente la connessione fra attività di soggetti differenti volte al perseguimento di un unico scopo e quindi funzionali, «inscindibilmente connesse» secondo la Corte ad individuare un'unica nozione di 'contesto'. Afferma la Corte: «le attività del gestore del motore di ricerca e quelle del suo stabilimento situato nello Stato membro interessato sono inscindibilmente connesse, dal momento che le attività relative agli spazi pubblicitari costituiscono il mezzo per rendere il motore di ricerca in questione economicamente redditizio e che tale motore è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività»[38].

La Corte può così concludere che «l'articolo 4, paragrafo 1, lettera a), della direttiva 95/46 deve essere interpretato nel senso che un trattamento di dati personali viene effettuato nel contesto delle attività di uno stabilimento del responsabile di tale trattamento nel territorio di uno Stato membro, ai sensi della disposizione suddetta, qualora il gestore di un motore di ricerca apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro».

Non diversamente su questo punto aveva argomentato l'avvocato generale, sottolineando come fosse necessario muovere dalla considerazione del modello economico dei fornitori di servizi di motore di ricerca su Internet[39].

[35] Così anche l'*UNCITRAL Model Law on Electronic Commerce*, art. 15 e il commento nella *Guide to Enactment*, par. 105 ss. In argomento v. L.G. Castellani, *I testi dell'Uncitral in materia di diritto del commercio elettronico*, in G. Finocchiaro-F. Delfini, *Diritto dell'informatica*, Utet, 2014, p. 43 ss. e G. Finocchiaro, *Il ruolo dell'Uncitral nello sviluppo della disciplina sul commercio elettronico*, *ibidem*, p. 63 ss.

[36] Così il punto 37 delle conclusioni dell'avvocato generale in *Weltimmo*.

[37] Parere n. 8/2010, pag. 10. V. anche le conclusioni dell'avvocato generale Jääskinen nella causa *Google Spain.*

[38] Così il punto 56 della sentenza Google Spain.

[39] Punto 64 e ss. delle conclusioni dell'avvocato generale. In particolare al punto 65:

L'interpretazione della Corte anticipa, quanto agli effetti, l'emanando regolamento europeo[40]. Secondo il testo della proposta di regolamento emendato attualmente disponibile, reso dal Consiglio dell'Unione Europea l'11 giugno 2015 (9565/15), il controverso art. 3 intitolato «Campo di applicazione territoriale» nella versione odierna dispone come segue: «Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione.

Il presente regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

a) l'offerta di beni o la prestazione di servizi ai suddetti residenti nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il controllo del loro comportamento, quest'ultimo inteso all'interno dell'Unione europea. […]»[41].

«dev'essere tenuto in considerazione il modello economico di un fornitore di servizi di motore di ricerca su Internet nel senso che il suo stabilimento ha un ruolo significativo nel trattamento dei dati personali se è collegato ad un servizio implicato nella vendita di pubblicità mirata agli abitanti di tale Stato membro». E al punto 67: «il trattamento di dati personali avviene nell'ambito di uno stabilimento del responsabile del trattamento se tale stabilimento funge da collegamento per il servizio di posizionamento per il mercato pubblicitario di tale Stato membro, anche se le operazioni tecniche di trattamento dei dati hanno luogo in altri Stati membri o in paesi terzi».

[40] In particolare sull'art. 3 della proposta di regolamento v. W. Kotschy, The proposal for a new General Data Protection Regulation—problems solved?, in International Data Privacy Law 2014, Vol. 4, No. 4, pp. 274-281.

[41] I considerando 20 e 21 aggiungono sul punto quanto segue.«20) Onde evitare che una persona fisica venga privata della tutela cui ha diritto in base al presente regolamento, è necessario che questo disciplini anche il trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono legate all'offerta di beni o servizi a dette persone indipendentemente dal fatto che vi sia un pagamento o no all'interno dell'Unione. Per determinare se tale responsabile del trattamento stia offrendo beni o servizi a dette persone nell'Unione, occorre verificare se risulta che il responsabile del trattamento intenda concludere affari con residenti in uno o più Stati membri dell'Unione. Se la semplice accessibilità del sito Internet del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica, di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il responsabile del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, e/o la menzione di clienti o utenti residenti nell'Unione, possono evidenziare l'intenzione del responsabile del trattamento volta all'offerta di beni o servizi a dette persone nell'Unione. 21) È opportuno che anche il trattamento dei

Nell'art. 3 dell'emanando regolamento si accentua la tendenza espansiva del diritto dell'Unione passando per l'individuazione di molteplici criteri di collegamento: quello territoriale (il luogo in cui viene effettuato il trattamento), ma assai estensivamente e poco chiaramente dilatato fino a comprendere l'ambiguo riferimento all'ambito delle attività' addirittura 'dell'incaricato'; quello teleologico (protezione dei residenti europei); quello che ha riguardo all'oggetto (fornitura dei servizi resi anche gratuitamente, così da ricomprendere, fra l'altro, i motori di ricerca); quello che ha riguardo agli effetti del trattamento (controllo del comportamento). Una pluralità di criteri, disomogenei e non chiaramente formulati, così da attrarre in ogni caso nell'ambito di applicazione della normativa europea i trattamenti anche all'estero effettuati.

3. Ulteriori indicazioni interpretative

Le decisioni della Corte passate in rassegna consentono di trarre alcune ulteriori indicazioni interpretative emergenti e inducono a riflettere su alcune conseguenze.

3.1 La pluralità di leggi nazionali applicabili

Nelle more dell'approvazione e dell'entrata in vigore del regolamento europeo, le decisioni della Corte conducono all'applicazione di una pluralità di leggi nazionali[42], conseguenza che si sarebbe voluta scongiurare nella prima versione della direttiva[43].

Addirittura si considera 'elusivo' il comportamento volto ad applicare la legislazione di un solo Stato membro, ovviamente attuativa della diretti-

dati personali di residenti nell'Unione ad opera di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al controllo del loro comportamento all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al 'controllo del comportamento' dell'interessato, occorre verificare se le operazioni che questi esegue su Internet sono sottoposte a tecniche di trattamento dei dati volte alla profilazione dell'utente, in particolare per prendere decisioni che li riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali».

[42] Lo ricorda l'avvocato generale nelle conclusioni relative al caso *Weltimmo*, punto 63, evidenziando una distanza considerevole fra le legislazioni degli Stati membri con riguardo alla regolamentazione e ai poteri sanzionatori delle autorità di controllo.

[43] Così ricorda L. Moerel, *Back to basics: when does EU data protection law apply?,* cit.

va[44]. Questo argomento è supportato dal considerando 19 della direttiva, il quale dispone che «quando un unico responsabile del trattamento è stabilito nel territorio di diversi Stati membri, in particolare per mezzo di filiali, esso deve assicurare, segnatamente per evitare che le disposizioni vengano eluse, che ognuno degli stabilimenti adempia gli obblighi previsti dalla legge nazionale applicabile alle attività di ciascuno di essi», dimostrando così palesemente quanta scarsa fiducia il legislatore europeo riponga in se stesso.

L'azione della Corte di giustizia rende più forte il diritto nazionale, in taluni casi a scapito della Commissione, come risulta evidente in *Schrems*, ove la Corte decide che spetti all'autorità irlandese decidere se occorre sospendere il trasferimento dei dati degli iscritti a Facebook verso gli Stati Uniti, sulla base dell'interpretazione dell'art. 8 della Carta dei diritti fondamentali ove è esplicito il riferimento all'autorità nazionale di controllo, ritenendo che le autorità nazionali di controllo possano *effettuare le proprie valutazioni anche quando vi sia già una decisione della Commissione.*

3.2 Distinzione fra 'dato personale' e 'valutazione'. Definizione di 'trattamento'

Ulteriori indicazioni interpretative vengono dalle decisioni in rassegna. In primo luogo, ancora alcuni chiarimenti sulla nozione di 'dato personale'.

La decisione del 17 luglio 2014, causa C-141/12, *Y.S. e a.* ha ad oggetto l'interpretazione degli articoli 2, lettera a), 12, lettera a), e 13, paragrafo 1, lettere d), f) e g), della direttiva 95/46/CE nonché degli articoli 8, paragrafo 2, e 41, paragrafo 2, lettera b), della Carta dei diritti fondamentali dell'Unione europea. Tale sentenza ha origine da due distinte domande pregiudiziali, poi riunite. In entrambi i casi, i cittadini di un paese terzo che hanno presentato una domanda di permesso di soggiorno temporaneo nei Paesi Bassi, contestano il rifiuto da parte del Ministero di trasmettere a detti cittadini copia di un documento amministrativo concernente le loro domande di permesso di soggiorno.

La Corte distingue fra dati personali e valutazioni effettuate nell'ambito di un procedimento amministrativo, in relazione alle quali non possono essere esercitati i diritti di accesso, rettifica e controllo previsti dalla direttiva sulla protezione dei dati personali. In particolare, stabilisce che l'articolo 2, lettera a), della direttiva 95/46/CE, dev'essere interpretato nel senso che i dati relativi al richiedente un titolo di soggiorno che compaio-

[44] Così la decisione *Weltimmo*, punti 28 e 30.

no in un documento amministrativo in cui viene esposta la motivazione addotta dal funzionario a sostegno della bozza di decisione che egli è incaricato di redigere nell'ambito del procedimento precedente all'adozione di una decisione relativa alla domanda e, eventualmente, i dati che figurano nell'analisi giuridica contenuta nel documento medesimo costituiscono dati personali ai sensi di tale disposizione, mentre detta analisi non può invece ricevere, di per sé, la stessa qualificazione. Infatti, l'analisi giuridica costituisce non già un'informazione riguardante il richiedente il titolo di soggiorno, ma tutt'al più, un'informazione riguardante la valutazione e l'applicazione, da parte dell'autorità competente, di tale diritto alla situazione del richiedente. Di conseguenza, contrariamente ai dati relativi al richiedente il titolo di soggiorno, l'analisi non può, di per sé, formare oggetto di una verifica della sua esattezza da parte di detto richiedente né di una rettifica ai sensi dell'articolo 12, lettera b), della direttiva 95/46/CE. Ciò considerato, il fatto di estendere il diritto di accesso del richiedente il titolo di soggiorno a detta analisi giuridica asseconderebbe, in realtà, non già l'obiettivo di tale direttiva consistente nel garantire la tutela del diritto alla vita privata del richiedente con riferimento al trattamento dei dati che lo riguardano, bensì quello di garantirgli un diritto di accesso ai documenti amministrativi, diritto che non forma tuttavia oggetto della direttiva 95/46/CE.

Si ribadisce, inoltre, una interpretazione estensiva della nozione di 'trattamento' in *Weltimmo,* confermando che va considerata 'trattamento'l'operazione consistente nel far comparire su una pagina Internet dati personali, come già in precedenza affermato dalla Corte di giustizia, *in primis* nel caso *Lindqvist* [45].

3.3 Bilanciamento fra il diritto all'accesso ai documenti amministrativi e il diritto alla protezione dei dati personali

Un'ulteriore tematica affrontata dalla Corte di giustizia in due delle sentenze sopra riportate (*Strack / Commissione* e *ClientEarth e PAN Europe / EFSA)*, concerne in particolare il bilanciamento fra il diritto all'accesso ai documenti amministrativi e il diritto alla protezione dei dati personali.

Costituiscono, infatti, oggetto della decisione le condizioni per il trasferimento di dati personali a norma dell'art. 8 del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei

[45] Così il punto 37 della sentenza *Weltimmo*.

dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati.

In questi casi, l'accesso ai documenti era stato accordato, ma oscurando alcuni dati personali. In particolare, nella seconda delle decisioni citate, erano stati oscurati i nominativi degli esperti che avevano formulato alcune osservazioni.

La Corte, in entrambe le sentenze, ricorda che ai sensi dell'articolo 8, lettera b), del regolamento n. 45/2001/CE, i dati personali possono, di norma, essere trasferiti soltanto se il destinatario dimostra la necessità della loro trasmissione e se non sussistono ragioni per presumere che possano subire pregiudizio interessi legittimi degli interessati.

Dalla stessa formulazione di tale disposizione emerge che essa subordina il trasferimento di dati personali al ricorrere di due condizioni cumulative. In tale contesto, incombe anzitutto a colui che chiede il trasferimento dimostrarne la necessità. Se la dimostra, spetta allora all'istituzione interessata verificare se non sussistano ragioni per presumere che il trasferimento in questione possa pregiudicare gli interessi legittimi dell'interessato. In assenza di ragioni di tale sorta, occorre procedere al trasferimento richiesto, mentre, nel caso contrario, l'istituzione interessata deve effettuare un bilanciamento tra i diversi interessi in gioco per pronunciarsi sulla domanda di accesso.

Tuttavia non può, in generale, riconoscersi alcuna automatica prevalenza dell'obiettivo di trasparenza sul diritto alla protezione dei dati personali. Rimane in capo alle parti richiedenti il trasferimento di dati personali l'onere di provare puntualmente e concretamente tale necessità. Allo stesso modo l'autorità interessata è tenuta a valutare se la divulgazione richiesta possa ledere concretamente ed effettivamente l'interesse protetto.

Ogni valutazione deve essere quindi effettuata caso per caso.

Sul bilanciamento fra diritti contrapposti si segnala anche la decisione del 16 luglio 2015, causa C-580/13, *Coty Germany*.

La domanda di pronuncia pregiudiziale verte sull'interpretazione dell'articolo 8, paragrafo 3, lettera e), della direttiva 2004/48/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale.

La domanda è stata presentata nell'ambito di una controversia tra la Coty Germany GmbH (in prosieguo: la «Coty Germany»), una società titolare di diritti di proprietà intellettuale, e la Stadtsparkasse Magdeburg, un istituto di credito, in merito al rifiuto di quest'ultima di fornire alla Coty Germany informazioni relative ad un conto bancario.

La Corte rileva che una disposizione del diritto nazionale che consenta un rifiuto di fornire dati personali in maniera illimitata, non contemplando alcuna condizione né precisazione è idonea a violare il diritto fondamentale di proprietà intellettuale e non rispetta, pertanto, l'esigenza di assicurare un giusto equilibrio tra i diversi diritti fondamentali controbilanciati dall'articolo 8 della direttiva 2004/48/CE, cioè diritto di proprietà intellettuale, da un lato, e diritto alla tutela dei dati personali, dall'altro.

Ne consegue che l'articolo 8, paragrafo 3, lettera e), della direttiva 2004/48/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, sul rispetto dei diritti di proprietà intellettuale, deve essere interpretato nel senso che esso osta ad una disposizione nazionale che consenta, in maniera illimitata ed incondizionata, ad un istituto bancario di opporre il segreto bancario per rifiutarsi di fornire, nell'ambito dell'articolo 8, paragrafo 1, lettera c), della medesima direttiva, informazioni relative al nome e all'indirizzo del titolare di un conto.

3.4 Trattamento dei dati personali da parte di un'autorità amministrativa. Obbligo di informativa

La decisione del 1° ottobre 2015, causa C-201/14, *Bara e a.*, concerne ancora il trattamento dei dati personali da parte di un'autorità amministrativa. Ivi si precisa che anche nel caso di comunicazione dei dati personali da un'amministrazione pubblica ad un'altra amministrazione pubblica, l'interessato deve essere informato. In particolare, gli articoli 10, 11 e 13 della direttiva 95/46/CE devono essere interpretati nel senso che essi ostano a misure nazionali che consentono a un'amministrazione pubblica di uno Stato membro di trasmettere dati personali a un'altra amministrazione pubblica, a fini di trattamento, senza che le persone interessate siano state informate né di tale trasmissione né del successivo trattamento.

3.5 Elementi biometrici dei passaporti e dei documenti di viaggio

Infine, nella decisione della Corte di giustizia del 16 aprile 2015, cause riunite da C-446/12 a C-449/12, *Willelms e a.*, le domande di pronuncia pregiudiziale vertono sull'interpretazione degli articoli 1, paragrafo 3, e 4, paragrafo 3, del regolamento (CE) n. 2252/2004 del Consiglio, del 13 dicembre 2004, relativo alle norme sulle caratteristiche di sicurezza e sugli elementi biometrici dei passaporti e dei documenti di viaggio rilasciati

dagli Stati membri, come modificato dal regolamento (CE) n. 444/2009 del Parlamento europeo e del Consiglio, del 6 maggio 2009, in particolare in merito al rifiuto da parte della amministrazione olandese di rilasciare ai ricorrenti un passaporto (C-446/12, C-448/12 e C-449/12) e una carta d'identità (C-447/12) se non sono rilevati contestualmente i loro dati biometrici.

In materia di trattamento dei dati biometrici dei passaporti e dei documenti di viaggio, nella sentenza *Schwarz* (C-291/12, EU:C:2013:670) la Corte aveva già dichiarato che l'uso e la conservazione dei dati biometrici ai fini precisati all'articolo 4, paragrafo 3, del regolamento (CE) n. 2252/2004 sono conformi ai requisiti di cui agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

Nel caso di specie la Corte chiarisce che suddetto regolamento non è applicabile alle carte d'identità rilasciate da uno Stato membro ai propri cittadini, come le carte d'identità dei Paesi Bassi, e ciò indipendentemente tanto dalla durata della loro validità quanto dalla possibilità di utilizzarle nel corso di viaggi effettuati al di fuori di tale Stato.

Conclusioni

Come si è anticipato, nelle decisioni della Corte di giustizia da *Google* a *Schrems* si legge chiaramente l'importanza strategica della protezione dei dati personali e la volontà di affermare la competenza della Corte ed il modello europeo. Questo fenomeno non sorprende ed anzi è nella natura delle cose che ogni giudice tenda ad affermare la propria competenza. Il tema che si affronta è cruciale anche con riguardo alla legge applicabile e alla giurisdizione su Internet più in generale, ancora non risolto, non essendo individuabile un soggetto politico legittimato a emanare le regole a livello globale[46].

L'attenzione della Corte è concentrata proprio sul diritto alla protezione dei dati personali su Internet e il diritto alla protezione della vita privata appare quasi una citazione di stile, l'inevitabile elemento di un'endiadi che tuttavia non suscita una particolare autonoma attenzione.

Non appare tanto la vita privata il bene che si vuole proteggere, quanto piuttosto le informazioni, e più o meno consapevolmente, il valore

[46] Sull'argomento si rinvia U. Draetta, *Internet nel diritto internazionale*, in G. Finocchiaro-F. Delfini, *op.cit.,* p. 3 ss. e a G. Finocchiaro, *Lex mercatoria e commercio elettronico*, in *Diritto di internet*, Zanichelli, 2008, p. 1.

economico ad esse connesso. Il diritto alla protezione dei dati personali è talmente pervasivo da superare agevolmente i confini della vita privata in senso stretto e da approdare nel minaccioso territorio della diffusione delle informazioni su Internet.

In effetti, la partita realmente aperta è proprio quella sulla *governance* di Internet[47].

L'azione politica della Corte di giustizia potrà forse condurre all'affermazione del modello europeo sulla protezione dei dati personali, ma ciò dovrebbe indurre ad una seria riflessione proprio su questo modello.

Esso, infatti, non soddisfa sotto molti aspetti e necessiterebbe di una revisione radicale, ben più ampia di quella contenuta nella proposta di regolamento. Tale modello attualmente si presta, infatti, ad un'applicazione meramente formalistica e poco sostanziale che facilmente si riduce ad un modulo di informativa e alla prestazione di un consenso vuoto e ineffettivo. Manca un'adeguata attenzione sulla sicurezza dei dati, incentrata sui dati e non sull'interessato, il quale spesso è debole sotto ogni profilo: culturale, economico, tecnologico e soprattutto di consapevolezza. Manca un'analisi di tipo economico sul modello che si adotta: non soltanto dal punto di vista del titolare del trattamento ma anche dal punto di vista del mercato europeo. Mentre imprese come Google o Facebook potranno facilmente adattarsi ad un più severo (e costoso) diritto europeo, non è chiaro quanto questo graverà sulle imprese europee.

Troppo poco spazio è lasciato al bilanciamento del diritto alla protezione dei dati personali con altri diritti pure costituzionalmente garantiti, quali il diritto alla libertà di espressione, il diritto di accesso ad Internet e la libertà di impresa. Mentre affermare il diritto alla protezione della vita privata può corrispondere ai valori e alla cultura europei, così come affermare il diritto all'identità personale, il diritto alla protezione dei dati personali in sé considerato (e privato del collegamento spesso solo retoricamente operato con la protezione della vita privata) è talmente ampio e pervasivo da rischiare di divenire poco comprensibile.

Ergere un muro intorno all'Europa, poi, può significare proteggerla, ma anche isolarla dal resto del mondo con l'effetto, già descritto da molti, della balcanizzazione di Internet.

Sono temi politici, appunto, che richiederebbero un altro e diverso tavolo di discussione.

[47] Su questo punto, in maniera chiara ed incisiva, F. Pizzetti, *Le Autorità Garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain. È tempo di far cadere il 'velo di Maya'*, in *Dir. Inf.* 2014, p. 805 ss.

Abstract

The paper summarizes the ECJs decisions on personal data protection, from Google Spain to Schrems.

It points out the main issues touched by these decisions focusing in particular, on the relevance of the rights to privacy and to protection of personal data as fundamental rights and on the applicable law.

What emerges from the analysis of the argumentative path followed by the Court on these issues is the intention to extend the scope of the European data protection law beyond European borders.

The paper draws a special attention to the political role assumed by the ECJ in this context in promoting the European model.

Salvatore Sica - Virgilio D'Antonio

Verso il Privacy Shield*: il tramonto dei* Safe Harbour Privacy Principles

Sommario: Premessa. – 1. Il trasferimento di dati tra Europa e Stati Uniti: dalla raccomandazione OECD alla direttiva 95/46/CE. – 2. I *Safe Harbour Privacy Principles*. – 2.1. I principi codificati. – 2.2. Le FAQ. – 2.3. Ambito di applicazione e «self certification scheme». – 2.4. La «supremacy clause» in favore del diritto statunitense. – 3. I poteri della *Federal Trade Commission*, quelli delle *Data Protection Authorities* europee e la responsabilità aquiliana. – Conclusioni: dai *Safe Harbour Principles* verso il *Privacy Shield*, passando attraverso *Schrems*.

Premessa

Con una evidente accelerazione dei negoziati indotta dalla sentenza Schrems, nei primissimi giorni di febbraio 2016, Stati Uniti ed Unione europea hanno raggiunto un nuovo accordo volto a regolare i flussi transfrontalieri di dati tra i due ordinamenti: si tratta del cd. «EU-US Privacy Shield». L'intesa nasce, dunque, sulle ceneri del precedente quadro di regole concordate, indicate generalmente come «Safe Harbour Privacy Principles», in vigore da oltre un decennio e, nell'ottobre 2015, ritenute dalla Corte di Giustizia EU non sufficientemente garantiste per la tutela della riservatezza dei cittadini europei.

I *principles* costituiscono indubbiamente la base di partenza anche dell'attuale *Privacy Shield*: essi trovavano il proprio fondamento giuridico immediato nella direttiva 95/46/CE, che, all'art. 25, comma 1, nell'affrontare la disciplina dei trasferimenti di dati personali oltre i confini dell'Unione Europea, impone, quale standard di tutela per gli interessati, che il paese importatore garantisca ai flussi di informazioni un «livello di protezione adeguato»[1].

[1*] Il presente contributo, pur se unitariamente concepito dai due autori, deve così essere attribuito nelle sue singole parti: S. Sica: Premessa e § 1 – V. D'Antonio §§ 2/3 e Conclusioni. Il diritto comunitario in materia di privacy si caratterizza per la progressiva elaborazione, dottrinale prima ancora che giurisprudenziale e legislativa, di un quadro di

Il trasferimento di dati personali dall'area giuridica europea verso paesi terzi è, da sempre, circondato da particolari garanzie, in ragione del fatto che l'esportazione extraeuropea dei dati personali finisce per comportare, nella maggior parte delle occasioni, la transizione delle informazioni da un'area giuridica ad elevato grado di protezione per il diritto alla riservatezza verso ordinamenti ove il *right of privacy* non è circondato dalle medesime garanzie[2].

La scelta di *policy* dell'Unione, sotto questo profilo, è stata quella di porsi quale modello forte di tutela della riservatezza, imponendo a qualunque esportatore di dati personali di origine comunitaria di confrontarsi con lo schema normativo europeo, garantendo alle informazioni in transito un livello di tutela particolarmente elevato, modellato appunto sul paradigma della direttiva 95/46/CE[3].

Tanto è avvenuto anche nei rapporti tra Unione Europea e Stati Uniti, nella misura in cui l'ordinamento statunitense, pur presentando una lunga e consolidata tradizione di tutela del *right to privacy*, è caratterizzato dall'assenza di una regolamentazione unitaria e generale in materia, con una congerie di interventi settoriali (di matrice federale e statale, nonché autoregolamentare). Tale impostazione complessiva dello scenario norma-

principi forti. Hanno contribuito, tra gli altri, nella dottrina italiana a delineare questo nucleo centrale di principi D. Messinetti, voce «*Personalità (diritti della)*», in *Enc. dir.*, Milano 1983, XXXIII, 355 ss.; P. Rescigno, voce «*Personalità (diritti della)*», in *Enc. giur. Treccani*, Roma, 1990, XXIII, 2 ss.; V. Zeno-Zencovich, voce «*Personalità (diritti della)*», in *Digesto civ.*, Torino, 1995, XIII, 430 ss.; S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 583 ss., nonché G. Alpa, *Diritti della personalità emergenti: profili costituzionali e tutela giurisdizionale. Il diritto alla identità personale*, in *Giur. merito*, 1989, 464 ss.

[2] Vedi P.M. Schwartz, *The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures, in 126 Harv. L. Rev.* 1966 (2012-2013), il quale, rispetto alla genesi dei Safe Harbour Principles, evidenzia che «*at the start of July 2000, the Commission released the final text of the «Safe Harbor Arrangement» and a series of supporting documents. That same month, the EU Parliament rejected the agreement in a nonbinding resolution before the Commission approved it on July 25, 2000*».

[3] In questi termini, A. Mantelero, Data protection ed attività di impresa. Verso dove guardano gli USA?, in Dir. Inf. 2011, 457 ss., il quale (a pag. 457) evidenzia come il modello comunitario «*grazie ad un'acuta scelta di strategia normativa,[sia]stato esportato al di fuori dei confini dell'Unione, adottato o usato come esempio per legislazioni di diverse nazioni, ed è divenuto in ogni caso parametro necessario di confronto*». Per una ricostruzione dell'evoluzione del concetto di privacy negli Stati Uniti, si vedano A. Baldassarre, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974; S. Rodotà, Tecnologie e diritti, Bologna, 1995, 19, e, più in generale, R.A. Posner, *Privacy, Secrecy, and Reputation,* in *28 Buffalo Law Rev.* 1 (1979), con approfonditi studi di matrice sociologica e comparatistica.

tivo, accompagnata dalla predilezione, soprattutto nei rapporti di consumo, per la valorizzazione dell'autonomia privata e della negoziabilità delle garanzie connesse alla tutela della riservatezza, contribuisce a determinare la non equipararabilità della protezione offerta dall'ordinamento USA ai rigorosi standard comunitari.

La necessità di definire un quadro organico di principi, in analogia con il modello europeo, pur nel contesto dell'approccio settoriale statunitense, portò all'elaborazione di una serie di regole generali che, ove rispettate dal singolo esportatore di dati personali dall'Europa verso gli Stati Uniti, avrebbe consentito allo stesso di superare la soglia di adeguatezza di tutela imposta dalla direttiva 95/46/CE[4].

Tali principi, definiti appunto «Safe Harbour Privacy Principles», venero poi cristallizzati con la decisione 2000/520, adottata dalla Commissione sulla base dell'art. 25, par. 6, direttiva cit., creando così una presunzione di adeguatezza di tutela in favore di quegli operatori statunitensi che si fossero impegnati, tramite specifica ed esplicita accettazione, al rispetto degli stessi[5].

Con l'adozione dello strumento dei *principles* (implementato tramite diversi documenti ulteriori tra i quali le *Frequently Asked Questions* - FAQ applicative, pubblicate dalla *Federal Trade Commission*) venne creato, pertanto, un vero e proprio 'ponte' preferenziale in favore delle organizzazioni americane, così da consentire e favorire il perdurare dello scambio di dati (anche nel contesto del medesimo gruppo industriale e, soprattutto, attraverso il *web*).

Dopo numerosi scricchiolii, tuttavia, questo 'ponte' è infine crollato il 6 ottobre 2015, quando la Corte di Giustizia, ponendo un tassello fondamentale in un dibattito iniziato già negli anni '80 dello scorso secolo, ha sancito, con la cd. «sentenza *Schrems*», resa nel caso C-362/14, l'invalidità della decisione 2000/520/CE della Commissione europea, facendo così cadere la presunzione di adeguatezza di tutela insita nel rispetto dei *Safe Harbour Principles* e tracciando una linea di cesura nei rapporti tra Stati Uniti ed Unione Europea nel quadro della promozione di strumenti di *soft-law* atti a regolare il trasferimento transfrontaliero dei dati[6].

[4] Tra gli altri, A. Bradford, *The Brussels Effect, in 107 Nw. U. L. Rev. I* (2012), nonché D. Scheer, *For Your Eyes Only – Europe's New High-Tech Role: Playing Privacy Cop to the World,* Wall St. J., Oct. 10, 2003

[5] Sul punto, sia consentito rinviare a V. D'Antonio, *Il trasferimento dei dati all'estero*, *comm.* sub *artt. 42 – 45*, in P. Stanzione – S. Sica (a cura di), *La nuova disciplina della privacy*, Milano, 2004, 155 ss.

[6] Sulle diversità di approccio alla materia dell'ordinamento comunitario e di quello statu-

1. Il trasferimento di dati tra Europa e Stati Uniti: dalla raccomandazione OECD alla direttiva 95/46/CE.

Il primo importante accordo internazionale sul tema della circolazione transfrontaliera di dati personali venne definito nel 1980 dall'Organizzazione per la cooperazione e lo sviluppo economico (OECD), con la raccomandazione del Consiglio che dettava le linee guida in materia di «*Protection of Privacy and Transborder Flows of Personal Data*»[7].

L'atto, di natura non vincolante, è stato emendato soltanto nel 2013[8] e traccia alcuni principi-chiave per il governo della *digital privacy* i quali, seppur sintetizzati in una fase di sviluppo ancora embrionale della cd. società dell'informazione, hanno sensibilmente influenzato i successivi sviluppi normativi registrati in materia.

La raccomandazione sancisce, in primo luogo, otto principi generali applicabili alle legislazioni nazionali, attinenti: *a*) la limitazione della raccolta di dati personali (liceità, idoneità, consenso dell'interessato); *b*) la qualità dei dati (pertinenza rispetto agli scopi, accuratezza, completezza ed aggiornamento); *c*) l'indicazione dello scopo della raccolta (tipologia, adeguatezza temporale); *d*) la limitazione dell'utilizzo (scopo per cui sono stati raccolti, consenso dell'interessato o ordine dell'autorità giudiziaria); *e*) le garanzie sulla sicurezza (misure ragionevoli contro ogni rischio di perdita, accesso non autorizzato, distruzione, uso, modificazione o divulgazione; *f*) la trasparenza; *g*) i diritti dell'interessato (comunicazione, accesso, motivi del diniego, rettifica); *h*) la responsabilità del *data-controller*[9].

Quanto al trasferimento transnazionale dei dati, l'OCSE invitava gli Stati membri ad adottare tutte le misure appropriate e ragionevoli per garantire un flusso ininterrotto e sicuro di dati, in conformità ai principi sopra menzionati ed alle legislazioni nazionali. Emerge, pertanto, una generale tendenza ad incentivare i traffici transfrontalieri di informazioni e, per converso, la precisa scelta di *policy* volta a non ostacolarne lo sviluppo con normative settoriali eccessivamente protettive[10].

---

nitense, si vedano C.J. Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press, 1992, nonché del medesimo Autore, *Regulating Privacy*, New York, 1992.

[7] OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 23 settembre 1980 - C(80)58/FINAL.

[8] OECD, 11 luglio 2013 - C(2013)79. Vedi ancora V. D'Antonio, *Il trasferimento dei dati all'estero*, cit., 160.

[9] Vedi B. Markesinis, Protecting Privacy, Oxford, 1999.

[10] Si veda ad es. *Guidelines Governing the Protection of Privacy and Transborder Flows of*

Soltanto qualche mese dopo l'adozione della raccomandazione, il Consiglio d'Europa ratificò la Convenzione sulla protezione degli individui con riguardo al trattamento automatico di dati personali (c.d. Convenzione di Strasburgo)[11].

La Convenzione ricalca i principi generali tracciati in sede OCSE (qualità del trattamento, tipologia dei dati, sicurezza, diritti dell'interessato, rimedi e sanzioni[12]), affermando poi, all'art. 12, la generale liceità dei trasferimenti di dati da un paese membro all'altro effettuati in ossequio alle precedenti prescrizioni, fatta eccezione per quei casi in cui le legislazioni nazionali non prevedano una protezione rafforzata per determinate categorie di dati o, ancora, il trasferimento sia diretto ad uno Stato che non abbia sottoscritto la Convenzione attraverso l'intermediazione fittizia di un paese aderente[13].

Come è noto, i provvedimenti appena menzionati hanno rappresentato l'*humus* all'interno del quale è maturato il sistema di principi che confluirà poi nella direttiva 95/46/CE: quest'ultima, infatti, prende le mosse proprio da tali primi sforzi regolamentativi e, con riguardo ai *transborder data flows,* detta il principio generale per cui ogni trasferimento è consentito soltanto qualora il paese terzo garantisca un «adeguato livello di protezione» (*ex* art. 25 e considerando 57 dir. cit.). In questo senso, l'elevato grado di tutela declamato al considerando 10 si estende, seppur temperato dal parametro dell'adeguatezza, anche al di fuori del territorio

Personal Data, cit., n. 18: «*Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection*».

[11] Council of Europe, *Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data*, 28 gennaio 1981, European Treaty Series - No. 108.

[12] *Ibidem*, artt. 4-11.

[13] *Ibidem*, art. 12: «*The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization transborder flows of personal data going to the territory of another Party. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2: a) insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection; b) when the transfer is made from its territory to the territory of a non Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph*».

dell'Unione, come d'altronde è stato ribadito dai giudici della Grande sezione nella sentenza in commento[14].

In effetti, la disposizione comunitaria dedicata ai flussi transfrontalieri di dati, sulla base del parametro dell'adeguatezza del livello di protezione garantito dal Paese terzo, identifica diversi percorsi che possono condurre alla verifica della sussistenza di siffatto livello di tutela[15]. In tal senso, se un ordinamento extraeuropeo presenta un grado di protezione adeguato «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona»[16], la Commissione può adottare, sulla base dell'art. 25, par. 6, della direttiva 95/46, una decisione che, in buona sostanza, 'certifichi' l'adeguatezza della tutela garantita ai dati personali dal Paese terzo[17].

Al contrario, per quegli ordinamenti che non presentino un livello di protezione adeguato ai sensi del comma 2 dell'art. 25 della direttiva 95/46, la Commissione avvia negoziati per porre rimedio alla situazione e, *medio tempore*, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati verso il paese terzo in questione.

All'esito dei negoziati previsti dalla normativa comunitaria e degli impegni eventualmente assunti in tale sede (come della legislazione nazionale o degli impegni internazionali del Paese terzo), la Commissione

[14] CGE Grande sez., 6 ottobre 2015, causa C-362/14, par. 66: *«In virtù delle considerazioni che precedono, si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato»*.

[15] Secondo quanto stabilito dall'art. 25, par. 2, direttiva 95/46, l'adeguatezza del livello di protezione garantito da un paese terzo è valutata – secondo un elenco non esaustivo (cfr. par. 70 della decisione) - con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.

[16] Così par. 71 della decisione.

[17] Peraltro, come ribadito al par. 50 della decisione, *«la constatazione se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuata […] vuoi dagli Stati membri vuoi dalla Commissione»*. In tema, vedi anche Riccardo e Rosario Imperiali, *Il trasferimento all'estero dei dati personali. Modalità e soluzioni contrattuali per il flusso dei dati nel mondo economico*, Roma, 2003, ed ivi ampi riferimenti di bibliografia.

può valutare positivamente il livello di tutela garantito ai dati personali ed adottare una decisione favorevole alla circolazione extraeuropea degli stessi.

In questo caso, come ribadito anche nella sentenza *Schrems*, gli Stati membri sono tenuti ad adottare tutte le misure necessarie per conformarsi alla decisione della Commissione, favorendo i trasferimenti di dati personali verso il Paese terzo da essa interessato.

Ora, nella disciplina dei flussi extraeuropei, una delle 'vie' principali è quella che conduce i dati personali verso gli Stati Uniti, ordinamento che, ove confrontato con quello comunitario sotto il profilo della tutela della riservatezza, presenta una serie di 'lacune' che conducono verso un giudizio di inadeguatezza da parte della Commissione europea. I motivi, altre alla già sottolineata differenza di approccio alla materia, sono molteplici: tra l'altro, la privacy non è computata nel novero dei diritti fondamentali come avviene nella Convenzione europea per la salvaguardia dei diritti dell'uomo all'art. 8. Il sistema normativo settoriale, proprio del modello USA, presenta, poi, sotto il profilo della tutela del contesto privato (il *Privacy Act*, di fatto, riguarda soltanto il trattamento dei dati da parte degli uffici governativi), una protezione della *individual privacy* non generale e complessiva, bensì segmentato e da completare sulla base delle previsioni particolari (anche di natura autoregolamentare) dedicate a specifici ambiti nei quali, statisticamente, risulta maggiore l'incidenza nella vita privata degli individui[18].

[18] Si pensi, ad esempio, al settore degli investimenti finanziari ed a quello delle assicurazioni. Come osservato, è fuor di dubbio che esistano profonde divergenze di vedute, in materia di tutela del *right of privacy*, fra Europa e USA, dovute principalmente alla diversità di tradizione giuridica ed al differente sviluppo storico della disciplina in tema di privacy. Fondamentale, nella storia della dottrina statunitense in materia, è lo scritto di S.Warren – L. Brandeis, *The Right to Privacy,* in *4 Harvard Law Rev.* 193 (1890). Di notevole interesse anche Westin, *Privacy and Freedom*, New York, 1967, ed E. Aldermann – C. Kennedy, *Right to privacy*, New York, 1995, nonché E. Lawson, voce «*Privacy*», in *Encyclopaedia of Human Rights*, 2ª ed., Washington, 1996, 1194. Gli Stati Uniti, in effetti, sono generalmente favorevoli all'associazione fra soluzioni di mercato e tutela giuridica mirata per settori di particolare delicatezza (ad esempio: dati relativi a minori, cartelle sanitarie, informazioni bancarie) con una visione generale del diritto alla riservatezza molto liberale; l'Unione Europea, al contrario, predilige la definizione di un solido quadro giuridico di riferimento che potenzi il diritto dei singoli di intervenire sui dati personali che li riguardano. Gli USA, infatti, nonostante siano fra le prime nazioni ad aver adottato norme a tutela della privacy contro gli abusi del settore pubblico (grazie al *Privacy Act* del 1974), risultano attualmente molto più restii ad affrontare i numerosi rischi per la riservatezza che possono venire dal settore privato. Basti pensare che dei ventiquattro Paesi membri che hanno adottato le Linee-guida in materia di privacy

L'assenza, dunque, non soltanto di un sistema di principi generali come quello comunitario (il cosiddetto sistema *«one size fits all»*), ma di una stessa normativa di settore in grado di tutelare a pieno i soggetti privati (non soltanto statunitensi, ma anche comunitari, nel caso di trasferimento dei dati personali oltreoceano) ha condotto, per aggirare l'insufficienza delle garanzie per la persona, all'adozione dei *Safe Harbour Principles*, confluiti nella decisione 2000/520 adottata ai sensi dell'art. 25, par. 6, direttiva 95/46[19].

dell'OCSE, nel 1980, soltanto gli USA e la Turchia non hanno ancora approvato norme di legge o compiuto passi significativi in vista dell'approvazione di norme generali di riferimento in materia di privacy.

[19] Va detto, ad ogni modo, che sebbene le divergenze tra i due sistemi giuridici sembrassero, dopo l'accordo, all'apparenza superate, recentemente ed ancor prima della sentenza Schrems, il confronto si è riacceso, riproponendo il concreto pericolo del blocco dei flussi di dati globali, dei rapporti commerciali e dello sviluppo del commercio elettronico. Il nodo fondamentale è dato dal fatto che una parte della dottrina (e dell'opinione pubblica) statunitense ritiene che la disciplina europea in materia, così come i principi elaborati in sede di accordo, possano pregiudicare un'ampia gamma di transazioni via web, di natura finanziaria o per altri scopi, compromettendo la possibilità per le imprese USA di commercializzare beni e servizi entro i confini dell'Unione. In tema, v. P. Swire, *Elephants and Mice Revisited: Law and Choice of Law on the Internet*, in 1*53 U. Pa. L. Rev.* 1975, 1986-87 (2005), nonché R. Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, in *54 Hastings L.J.* 1183 (2003).

2. I Safe Harbour Privacy Principles

Il lavoro di redazione dei *Safe Harbour Privacy Principles*[20] prende le mosse alcuni anni dopo l'entrata in vigore della c.d. direttiva privacy del '95 e vede impegnati il governo statunitense e le istituzioni comunitarie in una fitta trattativa della durata di circa due anni al cui termine, nel luglio del 2000, venne siglato l'accordo.

La finalità di questo *agreement*, come esplicitamente dichiarato dal *Department of Commerce* statunitense, è quella di «*diminish this uncertainty and provide a more predictable framework for such data transfers*», così da incoraggiare, promuovere e sviluppare il commercio internazionale e gli scambi commerciali fra Stati Uniti ed Unione Europea[21].

Il complesso di principi recepito nella decisione 2000/520/CE è destinato ad essere utilizzato esclusivamente da organizzazioni (non necessariamente imprese) statunitensi che intendano importare dati personali dall'Unione Europea al fine di conformarsi, giovandosi di un meccanismo presuntivo, al livello di protezione *adeguato* che la direttiva comunitaria

[20] U.S. Department of Commerce, *Safe Harbor Privacy Principles*, 21 luglio 2000, il cui testo completo è consultabile all'URL: http://www.export.gov/safeharbor/eu/eg_main_018475.asp/. La Decisione n. 2000/520 della Commissione europea si compone essenzialmente dei seguenti allegati: 1) i «Principi di approdo sicuro (*Safe Harbour*)», 2) le «Domande più frequenti (FAQ)», 3) l'«Applicazione (*enforcement*) dell'approdo sicuro», 4) il documento recante la «Tutela della riservatezza e risarcimento dei danni, autorizzazioni legali, fusioni, acquisizioni secondo la legge degli Stati Uniti», 5) e 6) un carteggio intercorso tra le Autorità governative degli Stati Uniti e la Commissione europea relativo a chiarimenti su specifiche questioni in materia di tutela della riservatezza. La decisione in parola è stata recepita, nell'ordinamento italiano, con la deliberazione del Garante Privacy del 10 ottobre 2001 n. 36 «*Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli Stati Uniti, effettuati in base ai «Principi di approdo sicuro in materia di riservatezza» applicati in conformità alle «Domande più frequenti» (FAQ) ed all'ulteriore documentazione allegata alla Decisione della Commissione europea del 26 luglio 2000, n, 2000/520/CE*» (pubblicato in G.U. n. 275 del 26/11/2001). Sul provvedimento di recepimento adottato dal Garante si vedano, tra gli altri, Guerinoni – Bascelli, *Trasferimenti di dati personali all'estero. Il nuovo quadro normativo nazionale e le nuove regole comunitarie, in I Contratti*, 7, 2002, 74 ss., e Stumpo, *Osservatorio di diritto comunitario: il trasferimento dei dati fuori dalla UE*, in *Dir. e prat. soc.*, 4, 2002, 23 ss.

[21] Vedi S. Simitis, *Einleitung: Geschichte - Ziele - Prinzipien [Introduction: History - Goals - Principles]*, in *Kommentar Zum Bundesdatenschutzgesetz [Commentary on the Federal Data Protection Law]* 77 ss. (Spiros Simitis ed., 7th ed. 2011). Più in generale, C. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, in *147 U. Pa. L. Rev.* 613 (1999).

impone per i flussi extraeuropei di informazioni[22].

Il sistema dei *Principles* si fonda, pertanto, sulla logica dell'adesione volontaria delle organizzazioni statunitensi ad un sistema disciplinare di tutela della privacy fondato su un nucleo minimo di principi tratti dalla direttiva 95/46/CE, funzionale a garantire ai cittadini europei, i cui dati vengano esportati oltreoceano, un livello di garanzie adeguato[23].

Il *Department of Commerce*, al fine di assicurare la corretta applicazione della decisione 2000/520, compila e rende disponibile al pubblico un elenco delle organizzazioni che abbiano deciso di aderire ai *Safe Harbour*, in modo da rendere riconoscibili le stesse tanto per i privati i cui dati saranno oggetto di trasferimento extraeuropeo, tanto per le autorità di controllo comunitarie[24].

2.1. I principi codificati

Il sistema dei *Safe Harbour Principles* si compone, innanzitutto, di 7 principi generali e 15 *frequently asked questions and answers* (FAQs), da

[22] Cfr. F. Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, in 48 *B.C. L. Rev.* 609, 684 (2007). Nel testo della decisione 2000/520/CE, opportunamente, al fine fi evitare qualsivoglia forma di incertezza interpretativa circa la porta applicativa dei principi, si chiarisce pure che «*because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in the Member States*».

[23] Come rivela A. Mantelero, Data protection ed attività di impresa, cit., 458 ss., la *Federal Trade Commission*, nell'ambito della propria competenza in materia di trattamento dati dei consumatori, ha adottato il c.d. «notice-and-choice model», caratterizzato dalla possibilità di un ampio ricorso a forme di consenso implicito. D'altronde, come evidenziato dalla stessa FTC nel documento «*Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*» del marzo 2012 (reperibile alla pagina web: https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers) «*the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand*». L'Autore evidenzia ancora come, sempre nell'ottica di un intervento minimo in materia di privacy, la FTC abbia altresì fatto ricorso il c.d. «*harm-based model*», rinunciando ad una tutela di portata generale del consumatore ed optando invece per un intervento di protezione calibrato su peculiari tipologie di danno potenziale («*physical security, economic injury, and unwanted intrusions into their daily lives*»). In tema, vedi anche A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007.

[24] Propone una lettura critica ai *Safe Harbour Privacy Principles*, con diverse proposte di modifica, D.R. Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement*, in *41 Case W. Res. J. Int. L.* 193 (2009).

leggere in combinato disposto ed in una logica di interpretazione complessiva che ne favorisca l'applicazione ed il concreto recepimento da parte delle organizzazioni americane.

Nel novero dei principi essenziali, è sancito, innanzitutto, un generale dovere di informazione in favore degli interessati (*notice principle*) assimilabile soltanto in parte a quello di cui agli artt. 10 e 11 della direttiva 95/46/CE. Tale informativa ha ad oggetto le finalità per cui vengono raccolte e utilizzate le informazioni, le modalità per contattare le organizzazioni in relazione ad eventuali quesiti o reclami, la tipologia dei terzi a cui vengono fornite le informazioni e, infine, le opzioni e i mezzi che le organizzazioni interessate pongono a disposizione dei singoli individui per limitare l'utilizzazione e la rivelazione delle informazioni.

L'importatore di dati statunitense è tenuto a garantire siffatta informativa secondo un linguaggio chiaro e in modo da attirare l'attenzione quando si tratti del primo invito a fornire informazioni personali oppure non appena ciò risulti successivamente possibile, ma comunque prima che l'importatore utilizzi o riveli per la prima volta a terzi siffatte informazioni per finalità diverse da quelle per le quali le stesse erano state originariamente raccolte[25].

Sotto l'enunciazione del principio del consenso (*choice principle*), al meccanismo giuridico dell'*opt-in* è affidato il trattamento dei dati sensibili[26], con la necessità, quindi, del consenso espresso dell'interessato («*affirmative or explicit choice*») in relazione alla rivelazione a terzi delle informazioni o alla utilizzazione delle stesse per finalità differenti rispetto a quelle originarie o successivamente autorizzate.

Per i dati comuni, al contrario, è sufficiente che l'importatore statunitense garantisca all'interessato meccanismi di consenso implicito (secondo il paradigma dell'*opt-out*, anche per la cessione a terzi). In sostanza, l'in-

[25] Tuttavia, «*it is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The Onward Transfer Principle, on the other hand, does apply to such disclosures*». Sul punto, interessanti sono le riflessioni offerte da P. M. Schwartz, *Feature, Preemption and Privacy*, in 118 *Yale L.J.* 902, 915 (2009).

[26] Per «*informazioni di carattere sensibile*», ai sensi dei *Safe Harbour Privacy Principles*, devono intendersi quelle relative alle condizioni mediche e sanitarie, all'origine etnica o razziale, alle opinioni politiche, alle credenze filosofiche o religiose, all'appartenenza a sindacati ed, infine, alla vita sessuale. Va evidenziato, inoltre, che andrà considerata di carattere delicato anche «*any information received from a third party where the third party treats and identifies it as sensitive*». In tema, di recente, P.M. Schwartz – D.J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, in 86 *N.Y.U. L Rev.* 1814, 1823 (2011)

teressato deve avere la possibilità di esercitare una vera e propria facoltà di rifiuto rispetto alla rivelazione a terzi dei propri dati personali, nonché in ordine all'utilizzazione degli stessi per fini incompatibili con quelli per cui le informazioni stesse erano state originariamente raccolte o con quelli successivamente autorizzati[27].

Analogamente al disposto dell'art. 12 della direttiva 95/46/CE, agli interessati è garantita, inoltre, facoltà di accesso ai dati (*access principle*), con il potere di rettifica, aggiornamento e cancellazione degli stessi, potere che può essere limitato soltanto in ipotesi particolari[28].

I principi di *notice* e *choice*, come codificati nei *Safe Harbour*, si applicano anche ai cd. trasferimenti successivi (*onward transfer principle*), allorché l'ente statunitense intenda trasferire i dati personali a terzi. Quando il terzo destinatario dei dati agisce in qualità di rappresentante, l'importatore, prima del procedere al trasferimento, deve accertarsi che il destinatario aderisca ai *Principles* o, comunque, rientri nel campo d'applicazione delle norme comunitarie in materia o, ancora, di altri modelli che garantiscano idonee tutele per gli interessati. In ultima analisi, l'organizzazione statunitense, al fine di procedere al trasferimento dei dati personali a terzi, può stipulare con questi ultimi un accordo scritto che comporti per gli stessi l'obbligo di offrire almeno «*the same level of privacy protection as is required by the relevant Principles*»[29].

In conformità ai principi cardinali codificati nella direttiva 95/46/CE, poi, all'importatore statunitense viene imposto il rispetto dei principi di sicurezza (*security principle*) ed integrità dei dati personali (*data integrity principle*). In particolare, con formula non lontana dal dettato dell'art. 17

[27] Cfr. K.A. Bamberger – D. Mulligan, *Privacy on the Books and on the Ground*, in 63 *Stan. L. Rev.* 247 (2011). Agli interessati, in ogni caso, dovranno essere forniti mezzi chiari, agevolmente riconoscibili in quanto tali, di rapida fruizione e di costo accettabile per esercitare la propria scelta: «*Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice*».

[28] Nei *Safe Harbour Principles*, difatti, si chiarisce che «Individuals must have access to personal information about them that an organization holds and be able to correct, amend, *or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated*».

[29] In relazione a possibili profili responsabilistici, a chiosa dell'enunciazione dell'*onward transfer principle*, viene specificato che «*if the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing*».

della direttiva privacy, l'importatore statunitense, ove detenga, aggiorni, utilizzi o diffonda informazioni personali deve adottare ragionevoli precauzioni per proteggerle da perdita ed abusi nonché da accesso, rivelazione, alterazione e distruzione non autorizzati. Inoltre, le informazioni personali devono risultare pertinenti ai fini per cui sono state raccolte od a quelli successivamente autorizzati dagli interessati: se ed in quanto necessario per tali fini l'ente statunitense deve assumere *«reasonable steps»* per garantire che i dati siano attendibili in funzione dell'uso che si prevede di farne, accurati, completi e aggiornati[30].

L'ultimo dei principi enunciati è quello di *enforcement*, inerente la predisposizione di meccanismi volti a garantire, in concreto, il rispetto dei *Principles*, la possibilità di ricorso per gli individui cui si riferiscono i dati che vedano lesi i propri interessi dal mancato rispetto dei principi medesimi, e la non impunità degli enti inadempienti[31].

Come è evidente, i sette principi codificati in sede di accordo USA – UE finiscono per imporre all'importatore americano di dati personali di matrice europea gli obblighi essenziali che la direttiva 94/46/CE prescrive in capo ai titolari di trattamento comunitari, con una sostanziale esportazione, unitamente ai dati personali, del modello europeo di disciplina del diritto alla riservatezza.

2.2. Le FAQ

Come osservato, i sette principi che costituiscono il nucleo dei *Safe Harbour Principles* devono essere letti, interpretati ed applicati unitamente alle 15 *Frequently Asked Questions and Answers* (FAQs), anch'esse recepite in sede comunitaria con la decisione 2000/520.

Le FAQ riguardano alcuni aspetti specifici dell'applicazione dei

[30] V. K.A. Bamberger – D. Mulligan, *Privacy on the Books and on the Ground*, cit., 256.
[31] Cfr. J. Reidenberg, *Privacy Wrongs in Search of Remedies*, in 54 *Hastings L.J.* 877 (2003). Nel testo dei *Safe Harbour*, quale soglia minima di *enforcement,* vengono identificati i seguenti meccanismi: *«(a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations».*

Principles ed, in particolare, *Sensitive data*, *Journalistic exceptions*; *Secondary liability*; *Investment banking and audits*; *The role of the data Protection Authorities*; *Self-certification*; *Verification*; *Access*; *Human resources*; *Article 17 contracts*; *Dispute resolution and enforcement*; *Choice - timing of opt-out*; *Travel information*; *Pharmaceutical and medical products* e *Public record and publicly available information*[32].

Nella prospettiva di un'analisi comparatistica, le regole operazionali emergenti dalle FAQ possono essere funzionali vuoi a completare quel processo di 'assimilazione' delle tutele garantite dall'ordinamento statunitense con il sistema di principi e regole desumibile dalla direttiva 95/46/CE, vuoi a marcare le differenze rispetto all'*acquis communautaire* maturato in materia di tutela della riservatezza.

È il caso, ad esempio, della FAQ 1, dedicata ai dati sensibili, che riprende diverse ipotesi codificate dall'art. 8, co. 2, della direttiva comunitaria ai fini dell'esenzione dal sistema dell'*opt-in choice* anche per i *sensitive data* o, ancora, della FAQ 2, che disciplina il delicato equilibrio tra riservatezza e *freedom of the press*, attribuendo comunque prevalenza al *First Amendment* della Costituzione americana. In maniera analoga, l'articolata serie di «questions and answers» che compongono la FAQ 8, in materia di diritto di accesso, contribuisce ad offrire all'interprete una sostanziale sintesi del quadro normativo comunitario consolidatosi sul punto, a partire dalla direttiva 95/46, come interpretata nelle decisioni della Corte di Giustizia e negli interventi delle autorità indipendenti nazionali.

In buona sostanza, dunque, molte delle FAQ che completano il sistema dei *Safe Harbour Principles* non rappresentano soltanto uno strumento interpretativo essenziale dei principi codificati nel 'ponte' UE-USA, ma contengono regole ulteriori e peculiari, funzionali, il più delle volte, ad esplicitare come, di là dalla distanza delle declamazioni astratte, le norme operazionali consolidatesi nelle prassi dei due ordinamenti possano essere estremamente simili[33]. In altri casi, come detto, la logica delle FAQ è inve-

[32] Per approfondimenti circa le FAQ e la portata applicativa delle stesse, Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor*, cit., 196.

[33] Secondo il noto principio euristico della *praesumptio similitudinis*, le soluzioni pratiche adottate da differenti ordinamenti si rivelano spesso assimilabili o sostanzialmente uniformi, anche a fronte di declamazioni di principio e concettualizzazioni generali che si presentano molto lontane le une dalle altre. In dottrina, per tutti, K. Zweigert – H. Kötz, *Introduzione al diritto comparato*, vol. I, Milano, 1998, 44, nonché R. Sacco, *Introduzione al diritto comparato*, Torino, 1992, 47 ss. Ha proposto, al contrario, il principio della *praesumptio dissimilitudinis*, P. Legrand, *The Return of the Repressed: Moving Comparative Legal Studies beyond Pleasure*, in *75 Tul. Law Rev.* 1048 (2001).

ce quella di offrire risalto a specificità sistematiche della regolamentazione della materia proprie degli Stati Uniti, che il *Safe Harbour system* comunque non va ad intaccare: si tratta dell'esplicitazione di un sostanziale argine a potenziali rischi di eccessiva europeizzazione delle prassi d'oltreoceano in materia.

Come detto, il quadro degli *USA-UE Safe Harbour*, oltre ai *Privacy Principles* ed alle FAQ, si completa con le lettere dalla *Federal Trade Commission* e del *Department of Trasportation* relative ai rispettivi poteri di *enforcement*, nonché con lo scambio di missive tra il *Department of Commerce* statunitense e la Commissione europea e, infine, con la decisione 2000/520/CE che – preso atto dell'accordo *Safe Harbour* e dei relativi allegati – certifica l'adeguatezza del livello di tutela garantito dall'ordinamento statunitense in ordine ai *transborder data flows*[34]. Il complesso di questi ulteriori documenti svolge, nella logica complessiva del sistema dei *Safe Harbour* e della demarcazione di confini rispetto all'influenza dell'ordinamento comunitario su quello statunitense in materia di tutela della riservatezza, una funzione interpretativa dei *Principles* assolutamente analoga a quella evidenziata in merito alle FAQ.

2.3. Ambito di applicazione e 'self certification scheme'.

La portata sostanziale dei *Safe Harbour Principles* incontra importanti limiti oggettivi rispetto al proprio ambito di applicazione, dal momento che la possibilità di aderire a questo sistema di principi è limitata esclusivamente alle organizzazioni statunitensi che operino nei settori sottoposti all'autorità della *Federal Trade Commission* o del *Department of Transportation*.

Questo comporta l'esclusione dai *Principles* di importanti operatori economici, che pure possono far ricorso a forme di massiccia importazione di dati personali: si pensi alle istituzioni finanziarie, comprese banche, casse di risparmio e unioni di credito[35]; alle assicurazioni[36]; ai vettori comuni di

[34] Cfr. C. Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, in *Privacy & Security L. Rep.* 215 (2012).

[35] Questo specifico ambito è soggetto ai regolamenti emanati dal *Federal Reserve Board, dall'Office of Thrift Supervision e dal National Credit Union Administration Board*

[36] Il *McCarran-Ferguson Act* (15 U.S.C. § 1011 et seq.), infatti, affida la regolamentazione delle attività assicurative ai singoli stati. Tuttavia, le disposizioni del *FTC Act* si applicano all'industria assicurativa «*nella misura in cui tali attività non sono regolate da leggi statali*». La *Federal Trade Commission*, dunque, è competente nel caso di pratiche

telecomunicazione (tra cui gli *Internet Service Providers*)[37] e di trasporti interstatali; ai vettori aerei[38] ed agli operatori del settore zootecnico[39].

Peraltro, visto che l'autorità della *Federal Trade Commission* è limitata alle pratiche sleali o ingannevoli in materia commerciale o collegata al commercio (*«in or affecting commerce»*), non ricadono nell'ambito di applicazione dei *Safe Harbour* tutte le forme di raccolta ed utilizzazione di dati personali a fini non commerciali, quali, ad esempio, la raccolta di fondi per attività caritatevoli.

Ancora, tali principi sono applicabili soltanto alle organizzazioni americane private che ricevono dati personali dall'Unione, mentre le autorità pubbliche non sono tenute al rispetto degli stessi[40].

Il meccanismo di applicazione dei *Safe Harbour Principles* è quello del *«self certification scheme»*, in base al quale l'operatore statunitense gode della presunzione di adeguatezza di tutela e può procedere all'importazione di dati personali dall'Unione Europea dalla data in cui autocertifica al *Department of Commerce* l'adesione ai principi[41].

sleali o ingannevoli poste in essere da società di assicurazione, nel caso in cui tali società non siano impegnate in attività assicurative. Ciò potrebbe comprendere, ad esempio, il caso di assicuratori che vendono informazioni personali sui loro assicurati a imprese di marketing diretto di prodotti non assicurativi.

[37] In questo caso, il *Communications Act* prevede che la disciplina del *«interstate and foreign commerce in communication by wire and radio»* sia rimessa all'autorità della *Federal Communications Commission* (FCC). Cfr. 47 U.S.C. §§ 151 e 152.

[38] In materia trova applicazione il *Federal Aviation Act* del 1958 ed i vettori aerei sono soggetti all'autorità del *Department of Transportation*.

[39] Rispetto a questi ultimi, il riferimento normativo è al *Packers and Stockyards Act* del 1921 (7 U.S.C. § 181 et seq.) ed ai poteri attribuiti al *Secretary of Agriculture*.

[40] Cfr. par. 82 della decisione.

[41] Si rinvia ancora a stesse, D.R. Leathers, *Giving Bite to the EU-U.S. Data Privacy Safe Harbor,* cit., 196. Come chiarito dalla FAQ 6, *«To self-certify for the Safe Harbor, organizations can provide to the Department of Commerce (or its designee) a letter – signed by a corporate officer on behalf of the organization that is joining the Safe Harbor – that contains at least the following information: 1. name of organization, mailing address, email address, telephone and fax numbers; 2. description of the activities of the organization with respect to personal information received from the EU; and 3. description of the organization's privacy policy for such personal information, including: a. where the privacy policy is available for viewing by the public, b. its effective date of implementation, c. a contact office for the handling of complaints, access requests, and any other issues arising under the Safe Harbor, d. the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy (and that is listed in the annex to the Principles), e. name of any privacy programs in which the organization is a member, f. method of verification (e.g. in-house, third party) and g. the independent recourse mechanism that is available to investigate unresolved complaints».*

L'impegno al rispetto dei *Principles* va ribadito con cadenza almeno annuale ed, anche se non rinnovato, non viene meno per quanto riguarda i dati ricevuti durante il periodo nel quale l'operatore ha goduto dei vantaggi del *Safe Harbour agreement*. Ai fini della dichiarazione di adesione ai *Principles*, l'organizzazione statunitense può attestare il rispetto dei principi tramite procedure di autovalutazione (*«self-assessment approach»*) oppure facendo ricorso a revisioni esterne (*«outside compliance reviews»*)[42].

L'autocertificazione dell'impegno ad adeguarsi ai principi comporta l'obbligo di applicare le relative regole ai dati importati sino a quando l'operatore continuerà a trattarli, anche se successivamente dovesse per qualsiasi motivo abbandonare il sistema dei *Safe Harbour*. Peraltro, l'operatore che accetta i principi non è tenuto ad applicarli indistintamente a tutti i trattamenti di dati personali che pone in essere, bensì esclusivamente a quelli che abbiano ad oggetto informazioni trasferite dall'Unione Europea dopo la volontaria adesione all'accordo[43].

Come sottolineato dalla Corte di Giustizia al paragrafo 81 della decisione *Schrems*, il ricorso, da parte di un Paese terzo, ad un sistema di autocertificazione non è di per sé contrario al requisito previsto dall'art.

[42] La FAQ 7 precisa che *«Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above. A statement verifying the self- assessment should be signed by a corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about non-compliance". Al contrario, nel caso di revision esterna, «such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor Principles that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of 'decoys' or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed should be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance»*.

[43] Per una riflessione sui possibili scenari configurati dalla sentenza Schrems nell'ambito della sovranità digitale v. V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in questo Volume.

25, co. 6, della direttiva 95/46/CE; tuttavia, l'affidabilità di un sistema siffatto finisce per fondarsi essenzialmente sulla contestuale predisposizione di meccanismi efficaci di accertamento e di controllo che consentano di individuare e sanzionare, nella prassi, eventuali violazioni delle norme che assicurano la protezione dei diritti fondamentali ed, in particolare, del diritto al rispetto della vita privata, nonché del diritto alla protezione dei dati personali[44].

Sino alla pronuncia della sentenza *Schrems*, l'adesione al complesso dei *Safe Harbour Privacy Principles*, attraverso l'omologazione in chiave europea garantita dalla già citata decisione della Commissione, consentiva in pratica alle imprese statunitensi che trattano dati personali importati dall'Europa di evitare il pericolo di veder bloccato il trasferimento su iniziativa di autorità amministrative indipendenti o giurisdizionali degli Stati membri UE, nel momento in cui avessero dovuto fondare il proprio giudizio sulle sole regole vigenti oltreoceano[45].

I *Safe Harbour Principles* hanno in sostanza operato una sorta di *by-pass* tra la tutela dei dati personali di stampo comunitario e il diverso approccio adottato negli Stati Uniti garantendo uno spostamento ininterrotto di dati dal primo al secondo ordinamento, svolto sia per fini commerciali che, come la vicenda *Snowden* insegna, per motivi di sicurezza nazionale. Nel corso dei quindici anni di vigenza dell'accordo, un numero maggiore ai 5000 organismi ha sottoscritto o ancora adesso ottempera all'accordo[46].

[44] Analoghe perplessità sono state formulate anche oltreoceano: vedi, ad esempio, P. Swire, *Why the Federal Government Should Have a Privacy Policy Office*, in *10 J. Telecomm. & High Tech. L.* 41, 46-47 (2012).

[45] Per quanto concerne i costi di adesione al *Safe Harbour framework, «an organization that is self-certifying its compliance with the U.S.-EU Safe Harbor Framework and/or the U.S.-Swiss Safe Harbor Framework for the first time on or after March 1, 2009 must remit a one-time processing fee of $200.00. An organization that has previously self-certified its compliance with the U.S.-EU Safe Harbor Framework and/or the U.S.-Swiss Safe Harbor Framework and is due to reaffirm its compliance with the Framework(s) on or after April 1, 2009 must remit an annual processing fee of $100.00 on or before the anniversary of the organization's original self-certification»* (tratto dalla pagina *web*: http://build.export.gov/main/safeharbor/eg_main_020436).

[46] La lista completa è disponibile all'URL: https://safeharbor.export.gov/list.aspx/.Va detto che, nella primissima fase di adozione dei *Safe Harbour Privacy Principles*, pochissime organizzazioni statunitensi decisero di aderireagli stessi e, tra i pochi aderenti, appena una decina appartenevano al settore delle imprese. Questa iniziale diffidenza comportò il legittimo sospetto che vi fosse addirittura carenza di reale sostegno politico nei confronti dei *Principles*. In sostanza, sino ai primi anni dello scorso decennio, la maggior parte delle transazioni di dati personali tra Europa e Stati Uniti era ancora affidata a non poco pressappochismo ed alla 'fuga' dalla disciplina della Direttiva 95/46/CE. Il cambiamento

In sintesi, il 'ponte transatlantico' creato dalla decisione 2000/520/CE (e momentaneamente chiuso dalla Corte di Giustizia) poteva apparentemente contare, sul piano operazionale, di due distinte 'falle' applicative insite nell'accordo stesso: da un lato, esso non si estende a precisi settori quali quello delle telecomunicazioni, dei servizi bancari e finanziari e del 'no-profit'; dall'altro, gli organismi investiti del compito di vigilare in territorio statunitense sulla sua attuazione sono il *Department of Transportation* (solo per ciò che concerne le compagnie aeree e l'emissione di biglietti) e, soprattutto, la *Federal Trade Commission* (FTC) la quale, come è stato ribadito numerose volte nel corpo della sentenza[47], svolge un'attività di controllo limitata a pochi settori del mercato delle informazioni, attività peraltro esclusivamente orientata verso la tutela del consumatore[48].

2.4. La «supremacy clause» in favore del diritto statunitense

Nella decisione *Schrems*, la Corte di Giustizia, nel percorso argomentativo che porterà all'annullamento della decisione 2000/520, evidenzia, in più occasioni[49], come uno dei profili di maggiore criticità dei *Safe Harbour Principles* sia legato alle ipotesi in cui l'applicabilità dei principi possa incontrare delle limitazioni derivanti dalla supremazia del diritto statunitense rispetto all'accordo[50].

---

di prospettiva è legato, senza dubbio, all'affermarsi dei colossi imprenditoriali della Rete, che operando a livello globale e transnazionale hanno ritenuto di adoperare lo strumento giuridico dei *Safe Harbour* per non correre il rischio di vedersi precluso un mercato fondamentale quale quello europeo. Vedi ancora P. Swire, *Elephants and Mice Revisited*, cit., 1990.

[47] V. ad es. CGE Grande sez., 6 ottobre 2015, causa C-362/14, cit., par. 89: *«A ciò si aggiunge il fatto che la decisione 2000/520 non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura. Come rilevato dall'avvocato generale ai paragrafi da 204 a 206 delle sue conclusioni, i meccanismi di arbitrato privato e i procedimenti dinanzi alla Commissione federale per il commercio, i cui poteri, descritti segnatamente nelle FAQ 11 figuranti all'allegato II a tale decisione, sono limitati alle controversie in materia commerciale, riguardano il rispetto, da parte delle imprese americane, dei principi dell'approdo sicuro, e non possono essere applicati nell'ambito delle controversie concernenti la legittimità di ingerenze nei diritti fondamentali risultanti da misure di origine statale».*

[48] V. Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting of U.S. Privacy Standards*, in *25 Yale J. Int. L.* I, 87 (2000).

[49] Si pensi, a titolo esemplificativo, ai paragrafi 83/89 della decisione. Nella dottrina statunitense, J. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, in *38 Hous. L. Rev.* 717 (2001).

[50] Per una riflessione sui possibili scenari configurati dalla sentenza Schrems nell'ambito della sovranità digitale v. V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems:*

Secondo quanto previsto dalle premesse ai *Principles*, infatti, l'adesione a tali principi può essere limitata: *a*) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia degli Stati Uniti; *b*) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione; oppure *c*) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili[51].

La Corte di Giustizia, con la sentenza *Schrems*, sottolinea come tutto l'impianto della decisione 2000/520 sia evidentemente assoggettato, in ordine alla sua applicazione concreta, al primato delle esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia statunitensi, «primato in forza del quale le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime»[52].

Di conseguenza, in forza dell'esistenza di questa sorta di «supremacy clause» in favore del diritto statunitense, i *Safe Harbour Principles* finiscono per esporre i dati personali importati negli Stati Uniti a possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, con conseguente compromissione dei diritti fondamentali dei soggetti interessati[53].

Ancor prima della pronuncia della Corte di Giustizia nello *Schrems*

la sovarnità digitale e il governo internazionale nelle reti di telecomunicazioni, retro questo Volume.

[51] Vedi F. Bignami, *European versus American Liberty*, cit., 684, nonché F.H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, in *80 Iowa L. Rev.* 431 (1995).

[52] Così par. 86 della decisione. Cfr. L. Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, in *21 Eur. J. Int. L.* 441 (2010).

[53] Peraltro, in conformità con la propria giurisprudenza precedente, la Corte di Giustizia sottolinea (par. 87) come «*a tal riguardo, poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (sentenza Digital Rights Ireland e a., C293/12 e C594/12, EU:C:2014:238, punto 33 e la giurisprudenza ivi citata)*».

case, questo specifico elemento di criticità era stato già ampiamente analizzato dalla Commissione in due comunicazioni al Parlamento ed al Consiglio risalenti al 2013 (rispettivamente nn. 846 e 847), ove si evidenziava come, tenuto conto dei 'punti deboli' individuati, il regime dei *Safe Harbour* non poteva continuare ad essere applicato secondo le attuali modalità e che, nonostante ciò, l'abrogazione dello stesso avrebbe compromesso in maniera rilevante l'attività di imprese operati sia in Europa che negli Stati Uniti[54].

D'altronde, l'incontrollata ed accertata ingerenza di matrice pubblicistica (in particolare ad opera dei servizi di *intelligence* statunitensi) nelle prerogative primarie dei cittadini comunitari si rivela assolutamente incompatibile con il quadro di principi animante la direttiva 95/46/CE, tanto più ove si consideri che la decisione 2000/520 non contiene alcun passaggio specifico dedicato all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale. Analogo silenzio si registra, nei *Principles*, rispetto all'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di matrice pubblicistica[55].

[54] Il riferimento nel testo, presente in diversi passaggi della sentenza Schrems (ad esempio, al paragrafo 90), è a COM(2013) *846 final («Rebuilding Trust in EU-US Data Flows»*, reperibile all'indirizzo http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf), ed a COM(2013) 847 *final («On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU»*, alla pagina *web* http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf), ambedue del 27 novembre 2013. Le due comunicazioni trovavano il proprio fondamento nella cooperazione tra Unione Europea e Stati Uniti in seguito alla rivelazione dell'esistenza, negli USA, di diversi programmi di controllo che comprendevano la raccolta e il trattamento su larga scala di dati personali. In particolare, tutte le imprese partecipanti al programma PRISM (un programma di raccolta di informazioni su larga scala), che consentono alle autorità americane di avere accesso a dati conservati e trattati negli USA, risultavano certificate nel quadro dei *Safe Harbour* e che siffatto sistema era perciò diventato, in dispregio dei principi di necessità e proporzionalità, una delle principali piattaforme di accesso delle autorità americane di *intelligence* alla raccolta di dati personali inizialmente trattati nell'UE (come evidenzia la Corte di Giustizia discorriamo di veri e propri colossi del mercato della comunicazione, come Google, Facebook, Microsoft, Apple, Yahoo).

[55] In tema, C. Bennett – C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, 2006, 127 ss. e ancora G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE, retro* in questo Volume.

3. I poteri della Federal Trade Commission*, quelli delle* Data Protection Authorities *europee e la responsabilità aquiliana*

La vigilanza sul rispetto dell'accordo, come visto, viene esercitata – almeno in prima battuta - dalla *Federal Trade Commission*, un organismo competente in materia di pratiche commerciali sleali o ingannevoli o, più in generale, che si concentra sull'utente inteso come centro di interesse di attività di tipo consumeristico[56].

In particolare, nel momento in cui un'organizzazione statunitense dichiari di aderire ai *Safe Harbour Principles*, accetta di sottoporsi, anche rispetto a questo specifico profilo, all'autorità della *Federal Trade Commission* ai sensi della *section* 5 del *Federal Trade Commission Act* (15 U.S.C., §§ 41-58).

Ne deriva che il mancato rispetto degli impegni assunti dall'importatore in ordine alla tutela della riservatezza venga equiparato, ai sensi della *section* 5, ad una pratica ingannevole[57]. Difatti, sebbene il sistema dei *Safe Harbour* si fondi su un meccanismo di adesione assolutamente volontario, ciò non esclude come gli operatori che intendano avvalersi della presunzione di garanzia di un livello di tutela adeguato, ai sensi della disciplina comunitaria, siano tenuti a dichiarare esplicitamente la propria volontà di tutelare le informazioni raccolte in conformità ai *Principles*, sicché la violazione di siffatto impegno costituisce *«deceptive practice»* ai sensi del *Federal Trade Commission Act*. Ad esempio, la rappresentazione ingannevole dei motivi per cui le informazioni vengono raccolte dai consumatori o delle modalità di trattamento dei dati personali può essere sanzionata dalla Commissione Federale quale pratica ingannevole in danno dei consumatori[58].

[56] Il *Department of Commerce* cura la tenuta di un elenco di tutti gli operatori che abbiano dichiarato di osservare i *Safe Harbour Principles*, aggiornandolo con cadenza annuale. In tema, W.E. Kovacic, *The Federal Trade Commission as Convenor: Developing Regulatory Policy Norms Without Litigation or Rulemaking*, in *13 J. on Telecomm. & High Tech. L.* 17 (2015) ed *ivi* ampi riferimenti bibliografici; e ancora G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in questo Volume, parr. 2 e ss. ..

[57] Per *«deceptive practice»*, ai sensi della section 5 del *Federal Trade Commission Act*, si intende *«a representation, omission or practice that is likely to mislead reasonable consumers in a material fashion»*. In tema, M. Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, in *Stan. Tech. L. Rev.* 1 (2001).

[58] Rispetto a questo profilo, interessanti spunti di riflessione sono in F.H. Cate, *The Failure of Fair Information Practice Principles, in Consumer Protection in the Age of the «Information Economy»* 341 (Jane K. Winn ed., 2006).

I poteri della *Federal Trade Commission* in materia di violazione dei *Safe Harbour* sono, allora, dettati dalla *section* 5 (ed, in particolare, dal 15 U.S.C. § 45)[59]: l'autorità dichiara l'illiceità di *«unfair or deceptive acts or practices in or affecting commerce»* e può porre in essere idonee misure *«to prevent such acts and practices»*, nonché pronunciare *«cease and desist orders»* al fine di far cessare violazioni già in atto.

Inoltre, per motivi d'interesse pubblico, la Commissione Federale ha facoltà di sollecitare la pronuncia da parte di una *District Court* di un *«temporary restraining order»* oppure di una *«temporary or permanent injunction»*[60] e, qualora vi sia stata ampia diffusione della pratica sleale o ingannevole o la FTC abbia già formulato ordinanze di cessazione e di desistenza in materia, può promulgare *«an administrative rule prescribing the acts or practices involved»*[61].

Ad esempio, con specifico riferimento alle attività di vigilanza sui trattamenti dei dati personali dei consumatori svolte nel corso degli ultimi cinque anni di vigenza dei *Safe Harbour Principles*, la *Federal Trade Commission* ha emanato numerosi ordini nei confronti dei principali *players* del settore della prestazione di servizi del cd. *web* 2.0.

Nell'ordine del marzo 2011 contro *Twitter*[62], la FTC ha rilevato, a seguito di un'articolata attività d'indagine, numerosi comportamenti non consentiti, richiamando espressamente la protezione della privacy dei consumatori. Il provvedimento ordina in primo luogo a *Twitter* di ottemperare in maniera adeguata ai doveri di trasparenza, informazione e sicurezza rispetto al trattamento delle cd. *«non public consumer informations»*, ovvero tutte quelle informazioni non rese pubbliche dall'interessato che ne consentano l'identificazione o ne indichino la provenienza (ad. es. e-mail, indirizzo IP, numero di telefono, informazioni prodotte attraverso canali di comunicazioni privati forniti dal prestatore).

In particolare, la FTC ha rilevato la sussistenza di pratiche atte a falsare la tutela della sicurezza, della privacy, della confidenzialità e dell'integrità

[59] Da sottolineare che chiunque non rispetti le ordinanze della *Federal Trade Commission* è soggetto a *civil penalty* fino a un massimo di $ 10.000, con ciascun giorno in cui l'inottemperanza persista costituente violazione a sé stante [cfr. 15 U.S.C. § 45(1)]. Allo stesso modo, chiunque infranga scientemente una regola dettata dalla Commissione Federale è passibile di *civil penalty* per $ 10.000 per ciascuna violazione [cfr. 15 U.S.C. § 45(m)]. Le azioni volte ad ottenere l'ottemperanza possono essere intraprese dal *Department of Justice* o, in alternativa, dalla stessa FTC (cfr. 15 U.S.C. § 56).

[60] Cfr. 15 U.S.C. § 53(b). Cfr. anche V. D'Antonio, *Il trasferimento dei dati all'estero*, cit., 165.

[61] Cfr. 15 U.S.C. § 57(a).

[62] FTC, In the Matter of Twitter Inc., 2 marzo 2011, docket no. C-4316.

delle informazioni non pubbliche, imponendo altresì al prestatore una serie di obblighi di adeguamento delle proprie prassi ai principi vigenti in materia di tutela della riservatezza.

L'ordine, che ha durata ventennale, dispone infatti il dovere di approntare e rendere effettivo un articolato programma di protezione dei dati non pubblici dei consumatori basato sull'individuazione di un responsabile del trattamento e sulla creazione di un apparato tecnico di tutela e salvaguardia (fondato sulla preventiva analisi dei rischi connessi). Il programma è sottoposto alla vigilanza ed al controllo (iniziale e poi a cadenza biennale) da parte di un organismo terzo e qualificato[63]; sul prestatore gravano altresì precisi doveri di *disclosure* nei confronti della Commissione[64].

Il provvedimento vincolante emesso contro *Twitter* è stato seguito da misure di tenore analogo che hanno interessato nell'ordine *Google*[65], *Facebook*[66] e *Myspace*[67].

In particolare, gli ordini ricalcano con maggiore dovizia di particolari le prescrizioni precedentemente descritte, adattandole agli specifici servizi

[63] I*n the Matter of Twitter Inc*, cit., p. 4: «*It Is Further Ordered that, in connection with its compliance with Paragraph II of this order, respondent shall obtain initial and biennial assessments and reports («Assessments») from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. […]*»

[64] *In the Matter of Twitter Inc*, cit., p. 5: «*It Is Further Ordered that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of: A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely-disseminated statements, including, but not limited to, statements posted on respondent's website that describe the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, with all materials relied upon in making or disseminating such statements, except that respondent shall not be required to provide any such statements that are made using the Twitter microblogging platform; B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that relate to respondent's activities as alleged in the draft complaint and any responses to such complaints; C. for a period of two (2) years from the date received, copies of all subpoenas and other communications with law enforcement entities or personnel, if such communications raise issues that relate to respondent's compliance with the provisions of this order; D. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order; and E. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment*».

[65] FTC, *In the Matter of Google Inc.*, 13 ottobre 2011, docket no. C-4336.

[66] FTC, *In the Matter of Facebook Inc.*, 27 luglio 2012, docket no. C-4365.

[67] FTC, *In the Matter of My Space LLC.*, 30 agosto 2012, docket no. C-4369.

offerti da ogni prestatore e rafforzando i concetti di trasparenza, consenso e sicurezza delle informazioni trattate con riguardo a tutte le tipologie di dati personali raccolte dai prestatori (cd. *covered information*[68]).

In questo senso, le misure comminate dalla FTC attraverso un approccio *case-by-case* hanno concorso a richiamare l'attenzione sull'efficacia vincolante di alcuni principi-chiave della tutela della riservatezza di stampo comunitario e sulle modalità di corretta ottemperanza agli stessi: a conferma di ciò, gli ultimi tre ordini vietano espressamente ogni forma di violazione e *misrepresentation* concernente accordi o programmi governativi volti a proteggere la privacy dei consumatori, tra i quali appunto viene citato il *Safe Harbour Framework*[69].

Sul versante europeo, la violazione dei *Principles* da parte di quelle organizzazioni statunitensi che hanno aderito agli stessi può comportare, indipendentemente dall'accertamento da parte della *Federal Trade Commission*, una sospensione dei flussi di dati personali.

Nello specifico, l'art. 3 della decisione 2000/520 prevede espressamente che le *Data Protection Authorities* nazionali degli Stati membri possano avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti verso un'organizzazione che abbia autocertificato la propria adesione ai *Safe Harbour Principles* sia quando vi sia stato l'accertamento di una violazione da parte degli organismi di controllo statunitensi, sia

[68] V. per tutti FTC, *In the Matter of Google Inc.*, cit., p. 3: «*'Covered information' shall mean information respondent collects from or about an individual, including, but not limited to, an individual's: (a) first and last name; (b) home or other physical address, including street name and city or town; (c) email address or other online contact information, such as a user identifier or screen name; (d) persistent identifier, such as IP address; (e) telephone number, including home telephone number and mobile telephone number; (f) list of contacts; (g) physical location; or any other information from or about an individual consumer that is combined with (a) through (g) above*».

[69] Si veda per tutti FTC, *In the Matter of My Space LLC*, cit., p. 2: «*It Is Ordered that respondent, and its officers, agents, representatives and employees, acting directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication: A. the extent to which respondent maintains and protects the privacy and confidentiality of any covered information, including, but not limited to: (1) the purposes for which it collects and discloses covered information, and (2) the extent to which it makes or has made covered information accessible to third parties. B. the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any other entity, including, but not limited to, the U.S.-EU Safe Harbor Framework*».

allorché sia soltanto molto probabile che i principi vengano violati. In quest'ultimo caso, tuttavia, devono sussistere pure *ragionevoli motivi* per ritenere che l'organismo di controllo statunitense non stia adottando o non adotterà misure adeguate e tempestive per risolvere il caso concreto, vi deve essere un rischio imminente di gravi danni per gli interessati in relazione alla continuazione del trasferimento dei dati ed, infine, l'autorità nazionale europea deve aver posto in essere procedure idonee, date le circostanze, ad informare l'organizzazione interessata, dando alla stessa l'opportunità di replicare alle censure.

Chiaramente, la sospensione del trasferimento transfrontaliero di dati personali deve cessare non appena l'ente abbia garantito il rispetto dei *Principles* e ciò sia stato notificato alle competenti autorità europee[70].

A chiosa delle riflessioni intorno alle conseguenze della violazione degli impegni assunti con l'accettazione dei *Safe Harbour Principles*, è necessario rilevare come, accanto ai profili pubblicistici appena evidenziati, possano ingenerarsi, in capo all'operatore 'infedele', anche conseguenze negative in termini risarcitori. In particolare, le organizzazioni aderenti ai principi di approdo sicuro potrebbero essere destinatarie di richieste di risarcimento danni collegate alla violazione della privacy (*breaches of privacy*), nonché essere ritenute responsabili di *misrepresentation* per non essersi attenute ai principi cui pure avevano dichiarato di conformarsi[71].

[70] La decisione 2000/520/CE, sempre all'art. 3, impone agli Stati membri di comunicare immediatamente alla Commissione l'adozione di misure restrittive alla circolazione di dati personali verso organizzazioni aderenti ai *Safe Harbour Principles* e, in ogni caso, gli Stati membri e la Commissione s'informano vicendevolmente in ordine ai casi in cui l'azione degli organismi di controllo statunitensi non garantisca la conformità ai principi negli Stati Uniti. Nell'ipotesi in cui si accerti che uno degli organismi incaricati di garantire la conformità ai *Principles* negli Stati Uniti non svolge la sua funzione in modo efficace, «*la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure secondo la procedura istituita dall'articolo 31 della direttiva 95/46/CE, al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione*».

[71] V. R.C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, in 77 *Calif. L. Rev.* 957 (1989). Il *Restatement of the Law, Second, Torts* § 525 prevede espressamente che «*One who fraudulently makes a misrepresentation of fact, opinion, intention or law for the purpose of inducing another to act or to refrain from action in reliance upon it, is subject to liability to the other in deceit for pecuniary loss caused to him by his justifiable reliance upon the misrepresentation*». Nell'ambito dei sistema dei *Safe Harbour Principles*, la *relevant representation* si identifica con la dichiarazione pubblica con la quale l'operatore statunitense si impegna a conformarsi ai principi in questione. Con l'assunzione di siffatto impegno, l'inosservanza consapevole dei principi potrebbe originare una richiesta risarcitoria per *misrepresentation* promossa da quanti hanno prestato fede alla falsa dichiarazione. Peraltro, poiché l'impegno ad attenersi ai principi è

Conclusioni: dai Safe Harbour Principles *verso il* Privacy Shield*, passando attraverso* Schrems.

In attesa della definizione del *Privacy Shield* (e della conseguente *adequacy decision* della Commissione), ad oggi, all'esito della pronuncia nel caso *Schrems*, la decisione 2000/520/CE inerente il riconoscimento dell'adeguatezza del livello di tutela garantito dall'ordinamento statunitense ai dati personali importati dall'Unione Europea è stata dichiarata invalida.

In particolare, la Corte di Giustizia, nel ribadire la propria esclusiva competenza in ordine al giudizio circa la validità delle *adequacy decisions* adottate ai sensi dell'art. 25, co. 6, della direttiva 95/46/CE[72], ha riconosciuto tuttavia che le *Data Protection Authorities* nazionali conservano il potere di esaminare le istanze di parte *ex* art. 28, co. 4, della direttiva cit., volte a far valere la non conformità dell'ordinamento terzo ai principi comunitari in materia di riservatezza[73].

Per quanto concerne lo specifico del sistema di trasferimento dei dati personali tra Europa e Stati Uniti introdotto dai *Safe Harbour Principles*, la *Schrems ruling* indica che l'opzione generale per un *self certification scheme* affidato all'adesione volontaristica degli operatori di settore non implica di per sé un giudizio di disvalore in termini di adeguatezza del livello di tutela

assunto nei confronti del pubblico in generale, anche i soggetti interessati e i responsabili del trattamento in Europa che trasferiscono dati personali all'importatore statunitense potrebbero intraprendere un'analoga azione legale nei confronti dello stesso. Cfr. anche P. Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in 57 *UCLA L. Rev.* 1701 (2010).

[72] Attualmente, le *adequacy decisions* adottate dalla Commissione hanno interessato Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. L'elenco completo è reperibile al seguente indirizzo *web*: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm/. Va detto, tuttavia, che sebbene la decisione *Schrems* sia limitata al vaglio dei *Safe Harbour Principles*, pressoché tutte le *adequacy decisions* di cui sopra presentano delle criticità analoghe a quella dichiarata invalida.

[73] Su questo specifico profilo, v. la *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, COM(2015) 566 final, del 6 novembre 2015, ove viene ulteriormente specificato che «*the Member States have to provide for the possibility to bring the case before a national court, which in turn can trigger the jurisdiction of the Court of Justice by way of a request for a preliminary ruling pursuant to Article 267 of the Treaty on the Functioning of the European Union (TFEU)*». Il testo completo della *Communication* è reperibile all'URL: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf/.

garantito ai flussi informativi, purché l'ordinamento terzo sia dotato di solidi ed efficaci meccanismi di rilevamento e di controllo che consentano, in concreto, di individuare e sanzionare eventuali violazioni.

Ebbene, proprio la carenza sotto questo specifico profilo dell'*enforcement* (soprattutto rispetto a possibili ingerenze di matrice pubblicistica sui dati), registrata dalla Corte di Giustizia, ha condotto alla dichiarazione dell'invalidità della decisione 2000/520/CE, con l'immediata conseguenza, in termini pratici, del venir meno della possibilità, per gli importatori statunitensi di dati personali, di fondare la legittimità del trasferimento di informazioni sulla sola base dei *Safe Harbour Principles*.

Allo stato, dunque, con il venir meno dell'*adequacy decision*, i trasferimenti di dati personali verso l'ordinamento statunitense sono, in linea di principio, vietati ai sensi dell'art. 25, commi 1 e 4, della direttiva 95/46/CE, con la necessità per gli operatori di ricorrere a strumenti alternativi, in particolare di matrice negoziale (*Standard Contractual Clauses* e *Binding Corporate Rules*)[74], sottoposti al vaglio delle *Data Protection Authorities* nazionali[75].

Ciò non toglie, tuttavia, che il paradigma proposto dalla decisione *Schrems* ai fini della valutazione di adeguatezza di tutela dell'ordinamento terzo, destinatario dei dati personali, porrà, nel prossimo futuro, non pochi problemi rispetto alla possibilità per la Commissione di definire un nuovo accordo quadro con gli Stati Uniti, assimilabile ai *Safe Harbour Principles*.

Difatti, nel momento in cui la formula «*adequate level of protection*» di cui all'art. 25 della direttiva 95/46/CE viene interpretata nel senso di esigere dal Paese terzo una soglia di tutela «*essentially equivalent*» a quella comunitaria, difficilmente un ordinamento giuridico, quale quello statunitense, ove la tutela del *right to privacy* non è circondata da quell'apparato generale di principi 'forti' tipico del diritto europeo, potrà introdurre correttivi tali soddisfare il vaglio di adeguatezza[76].

[74] È questa l'indicazione offerta dalla Comunicazione della Commissione COM (2015) 566 *final*, cit.

[75] Con uno specifico *advisory* pubblicato alla pagina http://www.export.gov/safeharbor/index.asp , lo *U.S. Department of Commerce* ha comunque chiarito che, anche dopo la decisione dell'ottobre 2015 della Corte di Giustizia, «*will continue to administer the Safe Harbor program, including processing submissions for self-certification to the Safe Harbor Framework*». Cfr. G.M. Riccio, *Model contract clauses e corporate binding rules: valide alternative al Safe Harbor agreement?* e ancora A. Mantelero, *Il trattamento dati nelle imprese nel post Safe Harbour. Strategie di breve, medio e lungo periodo*, infra in questo Volume.

[76] Va detto, ad ogni modo, che la Corte di Giustizia, al par. 73 della *Schrems ruling*,

In tal senso, le garanzie ulteriori che sono alla base dell'annunciato *Privacy Shield*, soprattutto se accompagnate, nell'ambito della cooperazione di polizia e giudiziaria in materia penale, da quanto previsto nell'accordo quadro volto a «rafforzare le garanzie di protezione dei dati nell'ambito della cooperazione fra autorità di contrasto», paiono tese a disegnare un insieme completo e armonizzato di garanzie per la protezione dei dati, che si applicheranno a tutti gli scambi transatlantici di informazioni personali.

In consonanza con quanto sancito dalla Corte di Giustizia, il *Privacy Shield*, diversamente da quanto previsto nel sistema *Safe Harbour*, prende le mosse proprio dalla necessità di uniformare il quadro di garanzie non soltanto nel contesto del settore commerciale ma altresì rispetto agli obblighi relativi all'accesso ai dati personali da parte delle pubbliche autorità, anche per esigenze di sicurezza nazionale.

Questo importante ampliamento della sfera di tutela garantita ai cittadini comunitari costituisce certamente un elemento di innovazione fondamentale nei rapporti tra USA e UE, che prende indubbiamente le mosse dal cuore della pronuncia *Schrems* e da uno dei profili maggiormente deficitari dei *Principles*.

Nella medesima direzione di rispetto delle regole enunciate nella decisione *Schrems* si muovono le ulteriori novità annunciate quali elementi caratterizzanti il *Privacy Shield*: rafforzamento dei meccanismi di vigilanza e *deterrence* a fronte di violazioni degli impegni assunti dalle imprese americane importatrici di dati, identificazione di limiti e garanzie chiare per quanto riguarda l'accesso alle informazioni da parte del governo degli Stati Uniti[77] e, soprattutto, la definizione di differenti mezzi di ricorso individuale, accessibili e di costo sostenibile, per i cittadini europei che ritengano i propri dati oggetto di uso improprio nel quadro del nuovo accordo. Accanto alla possilità di accesso gratuito ad organi di risoluzione alternativa delle controversie ed al ruolo di 'collettori dei reclami' individuali assegnato alle *Data Protection Authorities* nazionali, particolarmente

indica pure che, al fine di soddisfare il canone del livello di tutela adeguato, «*anche se gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione al fine di garantire il rispetto dei requisiti risultanti da tale direttiva, letta alla luce della Carta, tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione*». Vedi anche J. Reidenberg, *The Simplification of International Data Privacy Rules, in 29 Fordham Int. L.J.* 1128 (2006).

[77] Con istituzione, tra l'altro, di di un difensore civico («*Ombudsperson*»), cui i cittadini europei potranno rivolgersi in caso di uso improprio dei propri dati personali da parte delle Autorità di *intelligence* statunitensi.

interessante, rispetto a questo ultimo specifico profilo, si rivela la creazione di un *Privacy Shield Panel*, cioè un *«dispute resolution mechanism»* con il potere di assumere decisioni vincolanti nei confronti delle imprese americane aderenti all'accordo.

Sulla base di queste garanzie proprie del *Privacy Shield*, innovative rispetto al previgente quadro definito nel contesto dei *Safe Harbour Principles*, la Commissione si appresta ad approvare una nuova *adequacy decision*[78], volta ad attestare, in consonanza con quanto deciso dalla Corte di Giustizia in *Shrems*, che il livello di tutela garantito dal nuovo accordo EU-USA è equivalente agli standard europei di protezione dei dati personali.

Nel complesso, se la lettura degli elementi di innovazione contenuti nel *Privacy Shield* indica senza dubbio come vi sia stato un notevole passo in avanti rispetto alle garanzie in origine previste dai *Safe Harbour Principles*, ciò non toglie come la soluzione identificata sembri dettata più dall'esigenza di superare entro tempi ragionevolmente brevi la situazione di *empasse* conseguente alla sentenza *Shrems* che da una reale valutazione dell'adeguatezza dell'ordinamento statunitense, tanto più nell'ottica della soglia di tutela *«essentially equivalent»* richiesta dalla Corte di Giustizia.

Ed allora, anche alla luce delle prassi applicative che andranno a consolidarsi sul novellato quadro di principi definito dall'accordo e delle modalità di implementazione che dello stesso proporranno le autorità europee e quelle statunitensi, non è peregrino chiedersi quale potrà essere l'esito di un'eventuale futura valutazione del *Privacy Shield* da parte della Corte di Lussemburgo.

[78] Di cui, il 29 febbraio 2016, la Commissione ha rilasciato un primo *draft*, consultabile al *link* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf .

Abstract

As provided by article 25 of Directive 95/46/EC, the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if the third country in question ensures an adequate level of protection. In order to facilitate the data flows to United States, while ensuring a high level of protection of personal data, the Commission recognized the adequacy of the Safe Harbour Privacy Principles through the adoption of Decision 2000/520/EC. The paper analyzes the Safe Harbour framework, a set of principles, based on EU directive, issued by the U.S. Department of Commerce to provide adequate protection for the purposes of personal data transfers from the EU. Specifically, the Authors focus on genesis, content and criticalities of the Safe Harbour Principles, as well as the grounds for which the Court of Justice, in its judgment dated 6th October 2015, declared the Decision 2000/520/EC invalid.

Paola Piroddi

I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems *e nel nuovo regolamento generale sulla protezione dei dati*

Sommario: Considerazioni introduttive. – 1. Il quadro generale del trasferimento dei dati personali verso Stati terzi nella direttiva 95/46/CE. – 2. La decisione della Commissione relativa al «Safe Harbor» e il contesto fattuale del caso *Schrems*. – 3. La sentenza della Corte di giustizia: la 'piena indipendenza' delle autorità nazionali di controllo e la dichiarazione di invalidità della decisione della Commissione relativa al «Safe Harbor». Gli effetti della sentenza. – 4. La proposta relativa a una nuova decisione di adeguatezza della Commissione: il «Privacy Shield». – 5. I trasferimenti dei dati verso Stati terzi, le decisioni di adeguatezza della Commissione e i poteri delle autorità nazionali di controllo nel nuovo regolamento generale sulla protezione dei dati personali. – Conclusioni.

Considerazioni introduttive

Con la sentenza nel caso *Schrems c. Data Protection Commissioner*[1], la Corte di giustizia aggiunge un significativo tassello alla sua giurisprudenza volta ad adeguare alla Carta dei diritti fondamentali dell'Unione europea l'interpretazione della direttiva 95/46/CE, relativa alla tutela delle persone con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati[2].

Si tratta di una giurisprudenza evolutiva: infatti, quando è stata ema-

[1] Corte di giustizia dell'Unione europea (grande sez.), 6 ottobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, causa C-362/14, ECLI:EU:C:2015:650.

[2] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in *G.U.C.E.*, L 281 del 23 novembre 1995, p. 31 ss., modificata dall'all. II al regolamento (CE) 1882/2003 del Parlamento europeo e del Consiglio del 29 settembre 2003 recante adeguamento alla decisione 1999/468/CE del Consiglio delle disposizioni relative ai comitati che assistono la Commissione nell'esercizio delle sue competenze di esecuzione previste negli atti soggetti alla procedura prevista all'art. 251 Tr. CE, *ibid.*, L 284 del 31 ottobre 2003, p. 1 ss.

nata la direttiva, vent'anni fa, il diritto alla protezione dei dati personali non era ancora riconosciuto come diritto fondamentale nella Comunità europea. Questo diritto era tutelato soltanto nell'ambito del Consiglio d'Europa, in particolare dalla convenzione di Strasburgo n. 108 sulla protezione delle persone nel trattamento automatizzato dei dati di carattere personale[3], che all'epoca risultava già in vigore per diversi Stati membri della Comunità, e dall'art. 8 della Convenzione per i diritti dell'uomo e le libertà fondamentali («CEDU»), relativo al diritto al rispetto della vita privata e familiare[4]. Il diritto di 'ogni persona' alla protezione dei dati di carattere personale che la riguardano è stato introdotto nell'ordinamento giuridico dell'Unione europea soltanto dall'art. 8 della Carta dei diritti fondamentali[5] – peraltro inizialmente con efficacia dichiarativa e non vincolante. La Carta ha ottenuto «lo stesso valore giuridico dei trattati» solamente con il Trattato di Lisbona, che ha modificato l'art. 6, par. 1 TUE, e ha contestualmente riaffermato il diritto incondizionato alla protezione dei dati personali nell'art. 16 TFUE[6].

[3] Convenzione STCE n. 108, firmata a Strasburgo il 28 gennaio 1981, entrata internazionalmente in vigore il 1º ottobre 1985, per l'Italia il 1º luglio 1997 e per la Comunità europea il 15 giugno 1999 (v. *Amendments to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS no. 108) Allowing the European Communities to Accede*, adottati dal Comitato dei Ministri a Strasburgo il 15 giugno 1999). Si noti che la Corte europea dei diritti dell'uomo non esercita giurisdizione su questo strumento, aperto anche all'adesione di Stati non membri del Consiglio d'Europa. Cfr. anche il Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale, concernente le autorità di controllo ed i flussi transfrontalieri (STCE n. 181), firmato a Strasburgo l'8 novembre 2001, entrato in vigore il 1° luglio 2004. Su altri sviluppi internazionali del diritto alla protezione dei dati personali cfr. Ch. Kuner, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future*, in *Tilburg University Legal Studies Working Papers*, No. 16/2010, p. 9 ss.; L. Bygrave, *Privacy and Data Protection in an International Perspective*, in *Scandinavian Studies in Law*, 2010, p. 165 ss.

[4] Cfr., ad es., l'affermazione della Corte di giustizia nella sentenza 20 maggio 2003, Österreichischer Rundfunk, nelle cause riunite C-465/00, C-138/01 e C-139/01, in *Racc.*, 2003, p. I-4989 ss., par. 70: «La stessa direttiva 95/46, *pur avendo come obiettivo principale quello di garantire la libera circolazione dei dati personali*, prevede, al suo art. 1, n. 1, che «[g]li Stati membri garantiscono […] la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali'».

[5] Sull'art. 8 della Carta, cfr. P. Piroddi, *Art. 8 Carta dei diritti fondamentali dell'Unione europea*, in F. Pocar, M.C. Baruffi (a cura di), *Commentario breve ai trattati dell'Unione europea*, 2° ed., Padova, 2014, p. 1682 ss.

[6] Sull'art. 16 TFUE, che ha recuperato l'art. I-51 Tr. Cost., cfr. P. Piroddi, *Art. 16 TFUE*, in F. Pocar, M.C. Baruffi (a cura di), *Commentario breve* cit., p. 189 ss. In precedenza,

La giurisprudenza della Corte di giustizia ha contribuito in modo significativo all'evoluzione del diritto alla protezione dei dati personali come diritto fondamentale della persona nell'Unione europea, applicando all'interpretazione della direttiva 95/46/CE non soltanto l'art. 8 della Carta, ma anche il più consolidato diritto alla riservatezza, salvaguardato dall'art. 7 della stessa Carta e dall'art. 8 della CEDU nel quadro del diritto al rispetto della vita privata e familiare[7]. Basti ricordare, tra le sentenze più note di questa giurisprudenza, quella nel caso *Schecke e Eifert*[8]; la sentenza nel caso *Digital Rights Ireland*[9], che ha annullato la direttiva 2006/24/CE sulla conservazione dei dati generati o trattati nell'ambito dei servizi pubblici di comunicazione elettronica e di reti pubbliche di telecomunicazione; e infine la recente pronuncia nel caso *Google Spain*[10].

La sentenza *Schrems* si inserisce in questa giurisprudenza, che ultima-

l'art. 286 Tr. CE, inserito dal Tr. Amsterdam (*ex* art. 213B Tr. CE), aveva già stabilito l'applicazione della direttiva 95/46/CE alle istituzioni e agli organismi dell'Unione, e aveva previsto la nascita del «Garante europeo della protezione dei dati», formalmente istituito dall'art. 41 del regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, in *G.U.C.E.*, L 8 del 12 gennaio 2001, p. 1 ss.

[7] Cfr. Corte di giustizia, 9 novembre 2010, Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen, cause riunite C-92/09 e C-93/09, in Racc., 2010, p. I-11063 ss., par. 47 ss., nella quale la Corte mette in stretta relazione l'art. 8 CEDU e gli artt. 7 e 8 della Carta attraverso il riferimento all'art. 52, par. 3 e all'art. 53 della stessa Carta, creando in tal modo un anello di congiunzione tra la CEDU e il sistema di tutela dei diritti fondamentali proprio dell'ordinamento giuridico dell'Unione europea. Questo già prima dell'entrata in vigore del Trattato di Lisbona che, attraverso l'introduzione dell'art. 6, par. 3 TUE ha attribuito efficacia vincolante alla CEDU nell'Unione. Per un caso di applicazione del solo art. 8 CEDU alla direttiva 95/46/CE, v. Corte di giustizia, 20 maggio 2003, C-465/00, Österreichischer Rundfunk cit., par. 68. Per la giurisprudenza della Corte di giustizia che interpreta la direttiva 95/46/CE alla luce della Carta dei diritti fondamentali dell'Unione europea, cfr., per tutti, F. Bestagno, Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali, in Il dir. dell'Un. Eur., 2015, p. 25 ss.

[8] Corte di giustizia, 9 novembre 2010, *Schecke e Eifert* cit., spec. par. 52, 65. V. *supra*, nota 7.

[9] Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland Ltd et al. c. Minister for Communications, Marine and Natural Resources*, cause riunite C-293/12 e C-594/12, ECLI:EU:C:2014:238.

[10] Corte di giustizia, 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/12, ECLI:EU:C:2014:317, sulla quale si veda il volume monografico di *Dir. Inf.* n. 4-5 del 2014, e G. Resta, V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

mente sembra aver subito un'improvvisa accelerazione: la rapidità con la quale è stata decisa questa sentenza, pubblicata a pochissimi giorni di distanza dalla presentazione delle conclusioni dell'Avvocato generale[11], è inusuale per la Corte. Oltretutto, nel giro di una settimana, è stata pronunciata anche la sentenza nel caso *Weltimmo* e quella nel caso *Smaranda Bara*[12], tutte a seguito di rinvii pregiudiziali relativi all'interpretazione della direttiva 95/46/CE. Sembra che i giudici abbiano voluto affrettare la decisione dei casi ancora pendenti in questa materia, presumibilmente per approfittare dell'opportunità di poter ancora influire sul testo del nuovo regolamento generale di protezione dei dati[13]. Destinato a sostituire la direttiva nel quadro della riforma globale della disciplina relativa alla protezione ai dati personali nell'Unione europea, il regolamento si avvia infatti verso la conclusione dell'*iter* legislativo previsto per la sua approvazione. La Corte di giustizia, con la sentenza *Schrems*, sembra voler contribuire a definirne gli ultimi contorni ancora incerti.

[11] Conclusioni dell'Avv. gen. Y. Bot presentate il 23 settembre 2015, ECLI:EU:C:2015:627.

[12] Rispettivamente, sentenza 1° ottobre 2015, causa C-230/14, *Weltimmo*, ECLI:EU:C:2015:639; sentenza 1° ottobre 2015, causa C-201/14, *Smaranda Bara et al.*, ECLI:EU:C:2015:638.

[13] Cfr. la proposta relativa ad un regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, COM(2012)11 def. - 2012/0011(COD). Gli altri atti che fanno parte del «pacchetto» proposto dalla Commissione sono la comunicazione *Salvaguardare la privacy in un mondo interconnesso - Un quadro europeo della protezione dei dati per il XXI secolo*, COM(2012)9 def.; una proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati (COM(2012)10 def. – 2012/0010 (COD)), destinata a sostituire la decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (in *G.U.U.E.*, L 350 del 30 dicembre 2008, p. 60 ss.); e infine la relazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, basata sull'art. 29, par. 2, della decisione quadro 2008/977/GAI (doc. COM(2012)12, con l'allegato SEC(2012)75 def.), relativa all'attuazione di questa decisione negli Stati membri.

1. Il quadro generale del trasferimento dei dati personali verso Stati terzi nella direttiva 95/46/CE.

La direttiva 95/46/CE (nel prosieguo: la 'direttiva') definisce il quadro generale del trattamento dei dati personali nell'Unione europea, sia sotto l'aspetto relativo alla protezione dei diritti delle persone interessate, sia sotto l'aspetto relativo alla garanzia della libertà di circolazione di tali dati tra gli Stati membri dell'Unione e gli Stati membri dell'Accordo relativo allo spazio economico europeo[14]. Emanata sulla base giuridica delle norme del Trattato relative al ravvicinamento delle legislazioni[15], la direttiva persegue l'obiettivo di garantire la libertà di circolazione dei dati personali nel mercato interno attraverso l'armonizzazione delle garanzie nazionali di tutela della riservatezza rispetto al trattamento di questi dati.

Il principio generale stabilito da questo strumento è che gli Stati membri «non possono restringere o vietare la libera circolazione dei dati personali…, per motivi connessi alla tutela… dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali» (art. 1, par. 2 e 1). Il legislatore riteneva infatti che, per effetto del ravvicinamento delle legislazioni nazionali, la protezione equivalente dei diritti individuali non avrebbe più consentito agli Stati membri di ostacolare la libera circolazione di dati personali nel mercato interno per ragioni inerenti alla tutela delle persone fisiche[16].

Quando i dati delle persone residenti negli Stati membri sono trasferiti verso Stati terzi, il principio della libertà di circolazione è sostituito, nella direttiva, da un principio di autorizzazione condizionata: è consentito trasferire verso un Paese terzo i dati personali raccolti negli Stati membri dell'Unione soltanto se questo Stato garantisce un livello di protezione

[14] Infatti, la direttiva 95/46/CE è stata inserita nell'Accordo relativo allo «spazio economico europeo» («SEE/EEA») con l'art. 2 della decisione del Comitato misto SEE n. 83/1999 del 25 giugno 1999, che modifica il protocollo n. 37 e l'all. XI (servizi di telecomunicazione) dell'Accordo «SEE» (in *G.U.C.E.*, L 296 del 23 novembre 2000, p. 41 ss.). Inoltre, la direttiva è stata inclusa nell'all. B dell'Accordo del 26 ottobre del 2004 tra l'UE, la CE e la Confederazione svizzera (che non è Stato contraente dell'Accordo SEE, ma è parte dell'«Associazione europea di libero scambio», «AELS/EFTA»), riguardante l'associazione di quest'ultima all'attuazione, all'applicazione e allo sviluppo dell'*acquis* di Schengen (*ibid.*, L 53 del 27 febbraio 2008, p. 52 ss.).

[15] Art. 100A Tr. CE, ora art. 114 TFUE: v. il preambolo della direttiva.

[16] V. considerando 7, 8 e 9 della direttiva. Cfr., in proposito, le conclusioni dell'avv. gen. A. Tizzano presentate il 19 settembre 2002, nel caso *Bodil Lindqvist*, in causa C-101/01, in *Racc.*, 2003, p. I-12971 ss., par. 39.

'adeguato' dei dati stessi. Scopo di questa disposizione è evidentemente quello di evitare che la tutela garantita dal legislatore dell'Unione possa esser aggirata semplicemente trasferendo i dati verso Stati terzi con ordinamenti giuridici meno protettivi.

La direttiva tuttavia non definisce in cosa consista il 'trasferimento' di dati personali. In proposito, l'art. 25, par. 1 si limita a indicare che possono essere trasferiti tanto dati già trattati, quanto dati destinati a essere oggetto di trattamento nel Paese terzo nel quale vengono inviati. La Corte di giustizia ha apportato una significativa precisazione a questa nozione nella sentenza sul caso *Bodil Lindqvist*, che ha chiarito che l'inserimento di dati personali in una pagina di un sito *web* non configura un 'trasferimento' dall'Unione europea verso un Paese terzo ai sensi della direttiva, per il solo fatto di aver reso tali dati accessibili, attraverso un collegamento *internet*, a destinatari che si trovano fisicamente al di fuori dell'Unione europea[17]. In caso contrario, infatti, qualora cioè una pubblicazione *online,* di dati configurasse un 'trasferimento', ai sensi della direttiva, questo dovrebbe ritenersi indirizzato verso tutti quei Paesi terzi in cui esistono i mezzi tecnici per consentire di accedere alla pagina *web* attraverso un collegamento *internet*. Di conseguenza, ogni trasferimento di dati richiederebbe l'applicazione generalizzata della direttiva verso un numero indefinito di Stati (se non verso tutti), effetto certo non voluto dal legislatore. La Corte esclude quindi l'applicabilità della direttiva a quella specifica trasmissione di dati costituita dalla pubblicazione in un sito *web* accessibile anche da un Paese terzo, asserendo che non configura un 'trasferimento' di dati da un mittente a un destinatario, ai sensi della direttiva stessa.

È evidente che, con questa interpretazione, la Corte intende evitare di aggravare l'onere di *compliance* accollato al responsabile del trattamento che trasferisca dati verso Stati terzi attraverso un sito *web*[18]. Tuttavia, la

[17] Corte di giustizia, 6 novembre 2003, *Procedimento penale a carico di Bodil Lindqvist*, causa C-101/01, in *Racc*., 2003, p. I-12971 ss., par. 57 ss., spec. par. 71.

[18] Cfr. Y. Poullet, *Transborder Data Flows and Extraterritoriality: The European Position*, in *Journ. Intern. Comm. Law & Techn*., 2007, p. 141 ss., , il quale osserva (a p. 149) che la Corte utilizza un argomento non corretto sotto l'aspetto tecnico: infatti, essa considera come mittente di un trasferimento di dati che avvenga attraverso un collegamento *internet* ad un sito *web* non il *webmaster* (o, comunque, il creatore del sito), cioè la persona che ha caricato effettivamente i dati personali sulla pagina, ma l'*hosting provider*, cioè il soggetto che fornisce il servizio di rete che consiste nell'allocare il sito su un *server web*. Secondo la Corte non si configura un «trasferimento» di dati dall'Unione europea verso un Paese terzo ai sensi della direttiva, poiché i dati non vengono trasmessi *direttamente* dal mittente al destinatario, ma vengono caricati sul sito *web* da un soggetto terzo, cioè dall'*hosting provider*. Pertanto, senza che rilevi il fatto che il *server* dell'*hosting provider*

decisione della Corte non è esente da critica, a causa della sua motivazione: qual è infatti la differenza sostanziale fra 'trasferire' i dati da uno Stato membro ad uno specifico destinatario che si trovi in un Paese terzo (ad esempio, attraverso l'*e-mail*) e 'rendere accessibili' gli stessi dati allo stesso destinatario via *internet*, attraverso la pagina di un sito caricato sul *web* da un responsabile del trattamento stabilito in uno Stato membro[19]? È evidente che non vi è alcuna differenza sostanziale, ma soltanto l'utilizzo di un diverso mezzo tecnico.

La differenza ci sarebbe soltanto nel caso in cui il mittente (il *webmaster* del sito, responsabile del trattamento *ex* art. 2, lett. *d* della direttiva) non avesse la possibilità tecnica di restringere l'accesso al sito ai soli destinatari del trasferimento: cioè, nel caso in cui non potesse escludere dalla ricezione dei dati tutti coloro che non sono destinatari specifici del trasferimento[20]. È stato tuttavia osservato che in questo caso (eccezionale) verrebbe tuttavia in considerazione l'art. 4, par. 1, lett. *c* della direttiva[21], che prevede l'applicazione delle legislazioni nazionali di attuazione della direttiva al trattamento di dati personali effettuato per mezzo di «strumenti, automatizzati o non automatizzati», situati nel territorio degli Stati membri, anche se il responsabile del trattamento non è stabilito nell'Unione europea. È indubbio, infatti, che l'azione consistente nel caricare dati personali su una pagina di un sito *web*, effettuata da una persona che si trova in uno Stato membro dell'Unione, configuri l'utilizzo di «strumenti, automatizzati o non automatizzati», situati in tale Stato membro, a prescindere dal fatto che il *server* dell'*hosting provider* si trovi fisicamente in uno Stato membro o in uno Stato terzo. Di conseguenza, benché la Corte di giustizia escluda che la direttiva si applichi ad una trasmissione dei dati

si trovi fisicamente in uno Stato membro o in uno Stato terzo, la Corte esclude che in questo caso si verifichi un trasferimento, ai sensi della direttiva, il quale presupporrebbe una trasmissione diretta di dati da un mittente a un destinatario. In realtà, è evidente che l'*hosting provider*, che si limita a mettere a disposizione i mezzi tecnici per effettuare il trasferimento, è soltanto incaricato del trattamento, mentre responsabile del trattamento, anche rispetto alla trasmissione dei dati verso Paesi terzi, è e resta il *webmaster*, che assume la qualità di mittente del trasferimento, ai sensi della direttiva.

[19] Y. Poullet, *Transborder Data Flows* cit., p. 147.

[20] Così il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (Article 29 Data Protection Working Party, d'ora in avanti: «Gruppo Art. 29» o «WP29»), *Opinion 6/2002 on Transmission of Passenger Manifest Information and Other Data from Airlines to the United States*, WP66/02 del 24 ottobre 2002, p. 7; Id., *Opinion 4/2003 on the Level of Protection Ensured in the US for the Transfer of Passengers' Data*, WP 78/03 del 13 giugno 2003, p. 7.

[21] Y. Poullet, *Transborder Data Flows* cit., p. 149.

attraverso un sito *web* accessibile *online,* tuttavia, qualora il responsabile del trattamento non possa impedire l'accesso al sito a tutti coloro che non sono destinatari dei dati, questo trasferimento rientrerebbe comunque nell'ambito di applicazione della direttiva, attraverso l'art. 4, par. 1, lett. *c*.

Ai sensi dell'art. 25, par. 1 della direttiva, il trasferimento dei dati personali può avvenire soltanto a condizione che il Paese terzo verso il quale i dati sono trasmessi garantisca «un livello di protezione adeguato». L''adeguatezza' del livello di protezione dei dati esistente nello Stato terzo è dunque il requisito indispensabile per il trasferimento dei dati al di fuori dell'Unione europea. La direttiva tuttavia non definisce in cosa consista l''adeguatezza', né precisa quali siano le condizioni che consentano in concreto di ritenerla verificata. Dall'art. 25, par. 2 si evince soltanto che deve essere valutata caso per caso, in via preventiva, e «con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati». Tra le circostanze da prendere in considerazione, lo stesso par. 2 dell'art. 25 indica, in via esemplificativa e non esaustiva, «la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate».

Il Gruppo Art. 29, che ha più volte autorevolmente interpretato questa disposizione[22], ha sottolineato, nel cosiddetto *Methodology Paper*[23], come l''adeguata protezione' debba essere distinta da criteri simili, come quello di protezione 'sufficiente' o 'equivalente'. In particolare, l''equivalenza' esige la completa similarità legislativa, verificata da un rigoroso confronto analitico: richiederebbe quindi la trasposizione pura e semplice nell'ordinamento dello Stato terzo dei diritti, degli obblighi e dei meccanismi di protezione previsti nel sistema giuridico dell'Unione. L''adeguatezza', invece, si limita di per sé a richiedere soltanto la verifica che nell'ordinamento dello Stato terzo venga svolta la funzione di protezione richiesta, anche se in base ad elementi di natura diversa rispetto a quelli disposti dal

[22] WP29, *Discussion Document. First Orientations on Transfers of Personal Data to Third Countries. Possible Ways Forward in Assessing Adequacy*, WP 4/97 del 26 giugno 1997; Id., *Working Document. Judging Industry Self-Regulation: When Does It Make a Meaningful Contribution to the Level of Data Protection in a Third Country?*, WP7/98 del 14 gennaio 1998; Id., *Working Document. Preliminary Views on the Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries*, WP 9/98 del 22 aprile 1998.
[23] WP29, *Working Document: Transfers of Personal Data to Third Countries: Applying Art. 25 e Art. 26 of the EU Data Protection Directive*, WP12/98 del 24 luglio 1998.

legislatore dell'Unione[24].

La valutazione dell''adeguatezza' richiede quindi un approccio funzionale, che presuppone innanzitutto l'analisi preventiva dei rischi generati dallo specifico trasferimento, tenendo conto, in particolare, delle circostanze elencate dall'art. 25, par. 2 e, in generale, di tutte le circostanze nelle quali si svolge in concreto il trasferimento. Da questa analisi preventiva, si deve ricavare un criterio di verifica della conformità dell'ordinamento giuridico del Paese terzo ai principi essenziali di protezione dei diritti della persona, nonché un criterio di valutazione dell'effettività della tutela predisposta a tale scopo da questo Paese – fermo restando che questi appaiono come fini da raggiungere da parte dello Stato terzo, e non intaccano la sua libertà rispetto ai mezzi con cui raggiungerli. Il carattere adeguato del livello di protezione garantito da questo Paese deve essere infine determinato prendendo in considerazione tutte le misure, generali o particolari, di qualsiasi natura, legislativa, regolatoria o contrattuale, che appaiano disponibili in tale Paese per evitare gli specifici rischi che si sono evidenziati in relazione al quel concreto trasferimento[25].

A differenza di un astratto principio di equivalenza normativa, l'approccio funzionale all'adeguatezza dipende quindi dall'effettività della situazione esistente nell'ordinamento dello Stato terzo complessivamente considerato, ed esclude qualsiasi valutazione aprioristica: è stato detto che persino il fatto che uno Stato terzo abbia ratificato la convenzione di Strasburgo del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale non è di per sé una garanzia che questo Stato assicuri un'adeguata protezione, ai sensi della direttiva[26].

La direttiva non specifica nemmeno quale soggetto possa o debba valutare l'adeguatezza del livello di protezione riscontrabile nello Stato terzo, lasciando quindi la sua identificazione alla discrezionalità degli Stati membri in sede di implementazione della direttiva stessa. Alcuni Stati

[24] Y. Poullet, *Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données*, in *Juris-Classeur, Chronique*, 2003, p. 9 ss. (ora anche in M. Cools *et al.* (éds*), Ceci n'est pas un juriste. Liber Amicorum B. de Schutter*, Bruxelles, 2003, p. 242 ss.), a p. 10.

[25] Y. Poullet, *Pour une justification* cit., p. 12.

[26] Y. Poullet, *Transborder Data Flows* cit., p. 146. Cfr. anche, su questo metodo, Y. Poullet, B. Havelange, A. Lefebvre, *Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel. Rapport final* (*Centre de recherches informatique et droit, Université de Namur*, Belgium - *EU Commission*, DG XV), 1997, documento sulla base del quale il WP29 ha elaborato il «*Methodology Paper*» cit. *supra* (nota 23).

membri hanno previsto, ad esempio, che l'adeguatezza venga valutata anzitutto, con varie modalità, dallo stesso responsabile del trattamento che opera il trasferimento dei dati, talvolta sotto il controllo *ex post* dell'autorità garante nazionale. In questa prospettiva, è quindi possibile che il livello di protezione dei dati garantito dallo Stato terzo venga giudicato in modo diverso a seconda del soggetto tenuto ad effettuare la valutazione dell'adeguatezza, e a seconda dell'autorità che deve controllare tale valutazione. Tuttavia, la direttiva stabilisce che la Commissione può constatare con decisione, in conformità alla procedura istituita dall'art. 31, par. 2, che uno Stato terzo garantisce o non garantisce un livello di protezione adeguato. In entrambi questi casi, gli Stati membri sono tenuti a conformarsi alla decisione della Commissione, per espressa previsione dell'art. 25, par. 6 e par. 4 della direttiva – che, sotto questo aspetto, si limita evidentemente a confermare quanto disposto dall'art. 288 TFUE in relazione al carattere obbligatorio e vincolante della decisione come atto di diritto derivato dell'ordinamento dell'Unione europea.

Se la Commissione accerta che un Paese terzo offre un livello adeguato di protezione, il trasferimento dei dati personali dagli Stati membri verso tale Paese è consentito senza necessità di ulteriori garanzie o autorizzazioni particolari. Dall'entrata in vigore della direttiva a oggi, la Commissione ha emanato complessivamente dodici decisioni di adeguatezza *ex* art. 25, par. 6, alcune delle quali tuttavia di scarso o nullo significato economico e politico[27].

Qualora, viceversa, la Commissione dovesse constatare che uno Stato terzo non garantisca un adeguato livello di protezione (ad oggi, tuttavia, non risulta che l'abbia mai fatto), ogni trasferimento di dati personali verso il Paese terzo sarebbe vietato, in conformità al considerando 57 della direttiva.[28] Questo non è tuttavia un divieto assoluto: l'art. 26 consente, infatti, a determinate condizioni, di trasferire dati personali anche verso un Paese terzo che non garantisca un livello adeguato di tutela ai sensi dell'art. 25, par. 2[29], nonché verso un Paese terzo nei confronti del quale

[27] I Paesi interessati sono Andorra, Argentina, Canada, Fær Øer, Guernsey, Israele, Isola di Man, Jersey, Nuova Zelanda, Svizzera, Uruguay e Stati Uniti (limitatamente a *«The US Department of Commerce's Safe Harbor Privacy Principles»*, come si vedrà: cfr. *infra*, par. 3): v. l'elenco in *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*.

[28] In questo caso, ai sensi del par. 5 dell'art. 25, «la Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al par. 4».

[29] Cfr. WP29, *Working Document on the Protection of Individuals with Regard to the Processing of Personal Data* cit., p. 16 ss., 26 ss.

la Commissione non abbia preso espressamente alcuna decisione, né di adeguatezza, né di inadeguatezza.

Le deroghe consentite riprendono sostanzialmente le condizioni di legittimità del trattamento che sono oggetto dell'art. 7 della direttiva[30]: innanzitutto, i dati possono essere trasferiti qualora la persona interessata abbia espresso «in maniera inequivocabile» il proprio specifico consenso al trasferimento (art. 26, par. 1, lett. *a*); quando la trasmissione dei dati è necessaria per l'esecuzione di un contratto tra il responsabile del trattamento e la persona interessata, o per l'esecuzione di misure precontrattuali prese a richiesta della persona interessata (lett. *b*), oppure per la conclusione o l'esecuzione di un contratto concluso o da concludere, nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo (lett. *c*)[31].

Una seconda categoria di deroghe prende in considerazione specifiche categorie di flussi di dati: il trasferimento può essere disposto qualora sia necessario o imposto per la salvaguardia di un «interesse pubblico rilevante», o per l'esercizio di un diritto in giudizio (lett. *d*), o per la salvaguardia dell'interesse vitale della persona interessata, qualora l'interessato si trovi nell'incapacità fisica o giuridica di dare il proprio consenso (lett. *e*); oppure, ancora, qualora il trasferimento avvenga a partire da un registro pubblico, in presenza di determinate condizioni (lett. *f*).

Un'ulteriore deroga è prevista qualora «il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate» (art. 26, par. 2). È questo il caso delle «norme vincolanti d'impresa» («binding corporate rules» o «BCR»): codici di condotta, regolamenti interni e altri atti del genere, per mezzo dei quali le società si obbligano ad osservare, nell'ambito dei trasferimenti infragruppo, i principi di legittimità del trattamento. Ricadono in questa previsione, inoltre, le «clausole contrattuali tipo» («standard contractual clauses»),

[30] Ad eccezione della lett. *f* dell'art. 7, che dispone: «[Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando :] *f*) è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure del o dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona interessata, che richiedono tutela ai sensi dell'art. 1, par. 1».

[31] Non è quindi sufficiente l'esistenza di un contratto, o il riferimento ad un generico interesse di natura contrattuale: occorre la prova della necessità del trasferimento per concludere o per eseguire uno specifico contratto, o per adottare provvedimenti utili alla formazione del contratto.

oggetto di diverse decisioni della Commissione (par. 4 dell'art. 26)[32]. Ciascuna di queste deroghe prevede la necessità di specifiche autorizzazioni per il trasferimento di dati, che a loro volta presuppongono l'assolvimento di specifici adempimenti, tanto in sede europea, quanto in sede nazionale, ove richiesto dalle singole disposizioni legislative di attuazione della direttiva.

Sia pure con l'aggravio dovuto alle autorizzazioni richieste, i dati personali raccolti nell'Unione europea possono quindi essere trasferiti, in via di eccezione, anche verso Paesi terzi esplicitamente ritenuti inadeguati dalla Commissione, oppure verso Paesi terzi che non siano stati ritenuti né adeguati né inadeguati dalla stessa. Ma in presenza di una decisione di adeguatezza della Commissione le deroghe sono, in linea di principio, inapplicabili.

2. La decisione della Commissione relativa al «Safe Harbor» e il contesto fattuale del caso Schrems.

La vicenda che ha dato origine alla sentenza in commento prende avvio nel 2013, quando Maximillian Schrems, un cittadino austriaco utente di *Facebook*, propone un ricorso in Irlanda all'autorità garante per la protezione dei dati personali contro *Facebook Ireland* Ltd. Questa società, filiale europea della statunitense *Facebook* Inc., è responsabile del trattamento dei dati personali degli utenti del *social network* residenti o domiciliati al di fuori degli Stati Uniti e del Canada. Pertanto, *Facebook* Inc. è anche il responsabile del trattamento dei dati degli utenti residenti o domiciliati negli Stati membri dell'Unione europea. Come indica la Corte di giustizia nella sentenza[33], risulta che i dati raccolti da *Facebook Ireland* nell'Unione europea vengano abitualmente trasmessi, in tutto o in parte, alla casa madre americana. *Facebook* Inc. riceve quindi, in provenienza dall'Unione europea, un flusso continuo di dati, che sono già stati oggetto di elaborazione nel territorio di uno Stato membro, e che sono destinati ad essere oggetto di ulteriore trattamento nel territorio americano. Terminata questa attività, i dati sono archiviati per la conservazione in strutture fisi-

[32] La Commissione ha finora adottato quattro decisioni contenenti clausole contrattuali tipo (l'ultima delle quali, tuttavia, abroga e sostituisce una delle precedenti): v. tutte in http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

[33] V. par. 27 della sentenza.

camente ubicate sempre nel territorio degli Stati Uniti.

Il ricorso di Schrems non pone in questione la legittimità del trasferimento oltreoceano dei dati personali da parte di *Facebook Ireland*. Questa trasmissione, infatti, avviene in conformità ad una decisione di adeguatezza della Commissione *ex* art. 25, par. 1 e 6 della direttiva: la decisione 2000/520/CE[34], che ha dichiarato adeguato il livello di protezione dei dati personali trattati in conformità al sistema in essa previsto. Questa decisione ha dato esecuzione nell'ordinamento europeo ad un accordo concluso dopo anni di negoziati tra l'Unione e il «Department of Commerce» degli Stati Uniti, autorità equivalente ad un organo ministeriale a livello federale.

Questo accordo, denominato «Safe Harbor», o 'Approdo sicuro', stabilisce i principi sostanziali in materia di legittimità e riservatezza del trattamento dei dati applicabili nel trasferimento dei dati personali dall'Unione europea agli Stati Uniti, nonché gli orientamenti applicativi e i principi procedurali necessari per la sua esecuzione da parte degli Stati contraenti. L'accordo prevede, in sostanza, che le imprese private e le altre organizzazioni stabilite sul territorio americano che intendono ricevere dati provenienti dall'Unione europea, possano aderire volontariamente all'accordo, in pratica sulla base di un'autocertificazione, vincolandosi ad osservarne i principi alla luce degli orientamenti applicativi stabiliti nell'accordo stesso e assoggettandosi «all'autorità prevista per legge di un ente governativo degli Stati Uniti», compreso tra quelli indicati dall'accordo stesso – sostanzialmente, la *Federal Trade Commission* e l'*US Department of Transportation*. L'autocertificazione è resa esecutiva attraverso la notifica alla *Federal Trade Commission* e l'impegno relativo all'osservanza del «Safe Harbor» è pubblicizzato nelle forme previste dall'accordo stesso.

Le autorità di entrambi gli Stati sono obbligate a vigilare per garantire l'applicazione dell'accordo; negli Stati Uniti la competenza per l'esecuzione dell'accordo è attribuita sempre alla *Federal Trade Commission* e all'*US Department of Transportation*, i quali possono ricevere denunce, imporre la cessazione di eventuali violazioni dell'accordo, nonché disporre il risarcimento «di qualunque soggetto, a prescindere dal paese di residenza o dalla nazionalità, danneggiato a seguito del mancato rispetto dei

[34] Decisione della Commissione del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «*Domande più frequenti* (*FAQ*)» in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, in *G.U.C.E.*, n. L 215 del 25 agosto 2000, p. 7 ss.

principi applicati in conformità [all'accordo stesso]»[35]. I cittadini europei che intendano reclamare a causa del trattamento dei dati effettuato da un'impresa aderente al «Safe Harbor» devono quindi rivolgersi a tali enti amministrativi; soltanto in alcuni casi possono agire anche davanti a istanze giurisdizionali. Tuttavia, nel caso di uno specifico comportamento illegittimo da parte di un'impresa o di un'organizzazione aderente al «Safe Harbor», le autorità nazionali di controllo degli Stati membri dell'Unione europea possono interrompere il flusso dei dati diretto verso tale impresa o organizzazione (art. 3, par. 1 della decisione).

L'adesione all'accordo può essere limitata, da parte delle organizzazioni che vi partecipano, qualora ricorrano determinate condizioni, e in particolare: «*a*) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; *b*) [in presenza di] disposizioni legislative o regolamentari ovvero decisioni giurisdizionali, quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione»[36].

Non vi è necessità di sottolineare l'enorme importanza economica del «Safe Harbor»: nel corso del tempo, vi hanno aderito migliaia di imprese attive in tutti i settori economici, e in particolare i principali operatori del settore delle tecnologie dell'informazione e della comunicazione, *service providers*, motori di ricerca e *social media.* Tra questi, anche *Facebook* Inc., che quindi può legittimamente ricevere, trattare e conservare presso la sua sede negli Stati Uniti i dati personali di cittadini e residenti europei che siano stati trasferiti a partire da Stati membri dell'Unione. Il ricorso di Schrems non metteva in discussione la conformità del comportamento di *Facebook* Inc. al «Safe Harbor», sotto questo aspetto.

Quello che Schrems contestava nel suo ricorso, in realtà, era il giudizio reso dalla Commissione relativamente al livello di adeguatezza della protezione garantita dagli Stati Uniti nel quadro del «Safe Harbor». Il motivo erano le rivelazioni relative al cosiddetto scandalo «Datagate», effettuate da Edward Snowden, che aveva denunciato all'opinione pubblica l'attività di sorveglianza elettronica di massa perpetrata dai servizi di sicurezza americani, in particolare dalla *National Security Agency* («NSA»), nel quadro di un programma di intercettazioni denominato *PRISM*, attuato

[35] Art. 1, par. 2, lett. *b* della decisione della Commissione cit.
[36] All. I alla decisione della Commissione cit.

su larga scala e per lungo tempo negli Stati Uniti. Come si rileva dalle conclusioni della commissione d'inchiesta istituita dal Parlamento europeo e dalla risoluzione adottata dallo stesso Parlamento europeo alla chiusura dell'indagine[37], il programma *PRISM* aveva consentito alle autorità americane di *intelligence* di accedere in modo generalizzato e indiscriminato al contenuto di dati e metadati di traffico elettronico conservati nel territorio degli Stati Uniti, compresi i dati di cittadini europei, o di persone residenti nel territorio di Stati membri dell'Unione europea. Schrems rilevava nel suo ricorso che, poiché non era contestato che anche *Facebook* Inc. avesse collaborato a questo programma, i dati personali del suo *account* sul *social network*, una volta trasferiti in territorio americano, non erano e non sarebbero stati al riparo da gravissime forme di intercettazione, non consentite negli Stati membri dell'Unione europea. Doveva quindi ritenersi che gli Stati Uniti non fossero più in grado di garantire l''adeguata' protezione dei dati personali, contrariamente a quanto ritenuto dalla Commissione nella decisione relativa al «Safe Harbor».

La Commissione, in realtà, aveva riconosciuto, in alcune sue comunicazioni successive allo scoppio del «Datagate»[38], che l'applicazione del «Safe Harbor» da parte delle autorità americane era stata insufficiente sotto più punti di vista, e aveva quindi avviato trattative con le autorità americane per la rinegoziazione dell'accordo. Benché tali negoziati procedessero con lentezza, la Commissione si era astenuta dal sospendere la decisione di attuazione del «Safe Harbor», ritenendo che l'abrogazione *tout court* dell'accordo si sarebbe risolta in un danno per gli interessi degli operatori economici, tanto negli Stati Uniti, quanto nell'Unione. Malgrado la pendenza di tali negoziati, il «Safe Harbor» era quindi formalmente in vigore

[37] Cfr., rispettivamente, la relazione sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni (2013/2188(INI)), condotta dalla Commissione per le libertà civili, la giustizia e gli affari interni (rel. Moraes), doc. A7-0139/2014 del 21 febbraio 2014; e la risoluzione del Parlamento europeo del 4 luglio 2013 sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sulla vita privata dei cittadini dell'Unione europea e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni (2013/2682(RSP)) – P7_TA(2013)0322, entrambe in http://www.europarl.europa.eu.

[38] Cfr. le due comunicazioni della Commissione al Parlamento europeo e al Consiglio, l'una intitolata «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA», COM(2013) 846 def. del 27 novembre 2013, par. 3.2; e l'altra, relativa al funzionamento del regime 'Approdo sicuro' dal punto di vista dei cittadini dell'Unione europea e delle società ivi stabilite, COM(2013)847 def., sempre del 27 novembre 2013, spec. par. 7 e 8.

nell'ordinamento europeo nel momento in cui Schrems presentava il suo ricorso all'autorità irlandese di controllo dei dati.

L'*authority* rigettava tuttavia il ricorso, osservando, da un lato, che non vi era prova di uno specifico accesso da parte delle autorità americane ai dati personali del ricorrente, e rilevando, dall'altro lato, che la decisione della Commissione relativa al «Safe Harbor» era un atto obbligatorio e vincolante *ex* art. 288 TFUE, che richiedeva alle autorità nazionali di controllo degli Stati membri di conformarsi ad essa, finché fosse rimasta in vigore.

Schrems impugnava la decisione di rigetto davanti alla *High Court* irlandese. Quest'ultima osservava che, poiché non risultava che *Facebook* avesse trasgredito i suoi obblighi di osservanza del «Safe Harbor», l'autorità irlandese di controllo non avrebbe potuto interrompere il trasferimento dei dati verso gli Stati Uniti: infatti, come si è visto, l'art. 3, par. 1 della decisione della Commissione consente di sospendere l'accordo nei confronti di un soggetto che abbia aderito al «Safe Harbor» soltanto in presenza di uno specifico comportamento illegittimo.

Ciononostante, la *High Court* esprimeva forti dubbi sul fatto che il trasferimento dei dati verso gli Stati Uniti potesse ancora esser ritenuto compatibile con la direttiva. L'intercettazione dei dati da parte dell'autorità pubblica può infatti rispondere a legittimi obiettivi di interesse generale, quali la salvaguardia della sicurezza nazionale, della difesa, della pubblica sicurezza, o la prevenzione del terrorismo e di altri crimini. Queste eccezioni possono effettivamente giustificare una restrizione al diritto fondamentale alla tutela dei dati personali, come prevede anche l'art. 13, par. 1 della direttiva[39], ricalcando in buona parte i limiti consentiti dall'art. 8, par. 2 CEDU al diritto al rispetto della vita privata. Tuttavia, l'attività di sorveglianza praticata su larga scala dalle autorità americane sembrava aver ecceduto, secondo la Corte irlandese, la necessaria proporzionalità nel perseguimento di tali obiettivi, senza che oltretutto agli interessati fosse stata concessa un'adeguata garanzia di tutela giurisdizionale o amministrativa.

La *High Court* chiedeva quindi alla Corte di giustizia di pronunciarsi in via pregiudiziale sulla questione se, in presenza di una decisione della Commissione che dichiara 'adeguato' il livello di protezione dei dati personali garantito da uno Stato terzo, le autorità nazionali di controllo siano «assolutamente vincolate» a tale valutazione, o se possano discostarsene, ai fini dell'esame del ricorso di un cittadino europeo che asserisce che il livello di protezione in detto Stato terzo, nel quale sono stati trasferiti i suoi

[39] Cfr. in particolare le lett. *a, b, c* ed f dell'art. 13, par. 1.

dati, è inadeguato, alla luce di sviluppi fattuali e giuridici successivi alla decisione della Commissione[40]. Nell'ambito di tali sviluppi, la *High Court* includeva anche l'entrata in vigore della Carta dei diritti fondamentali dell'Unione europea, che tutela sia il diritto alla riservatezzaa e il diritto alla protezione dei dati personali (artt. 7 e 8), sia il diritto ad un ricorso effettivo e a un giudice imparziale (art. 47).

3. La sentenza della Corte di giustizia: la 'piena indipendenza' delle autorità nazionali di controllo e la dichiarazione di invalidità della decisione della Commissione relativa al «Safe Harbor». Gli effetti della sentenza

In conformità ad una giurisprudenza che può ritenersi ormai consolidata, come si è osservato, la Corte di giustizia risponde al rinvio pregiudiziale interpretando la direttiva alla luce degli artt. 7, 8 e 47 della Carta[41]. In base a questa interpretazione, i giudici dichiarano che una decisione di adeguatezza della Commissione *ex* art. 25, par. 6 della direttiva non può impedire alle autorità nazionali di controllo dei dati di esaminare, «con tutta la diligenza richiesta», la domanda proposta da una persona fisica a motivo della violazione dei suoi diritti relativi al trattamento dei dati personali, qualora i suoi dati siano stati trasferiti verso uno Stato terzo nel quale di fatto non venga garantito un appropriato livello di tutela. Inoltre, malgrado la questione non fosse oggetto di rinvio[42], la Corte dichiara invalida la decisione della Commissione relativa al «Safe Harbor». Su entrambi i punti della decisione, la sentenza aderisce alle conclusioni esposte dall'Avvocato generale, pur discostandosene occasionalmente nella motivazione.

La decisione sul primo punto, relativo all'obbligo delle autorità di controllo di ricevere i ricorsi individuali che contestano una decisione di adeguatezza della Commissione, è motivata dalla Corte in base alla 'piena indipendenza' delle autorità nazionali di controllo dei dati, indipendenza volta a consentire a tali autorità di esercitare effettivamente le funzioni

[40] V. par. 36 della sentenza.

[41] Sugli artt. 7, 8 e 47 della Carta v., rispettivamente, C. Campiglio, *Art. 7*, P. Piroddi, *Art. 8* e M. Castellaneta, *Art. 47*, tutti in F. Pocar, M.C. Baruffi (a cura di), *Commentario breve* cit., rispettivamente a p. 1678 ss., 1682 ss., 1770 ss.

[42] Per un precedente nel quale la Corte ha trasformato di fatto un rinvio pregiudiziale di interpretazione in rinvio pregiudiziale anche di validità, occorre risalire a Corte di giustizia, 1° dicembre 1965, *Schwarze*, causa 16/65, in *Racc.*, 1965, p. 910 ss.

loro attribuite dall'art. 28 della direttiva[43]. Afferma la Corte che lo *status* di indipendenza delle autorità di controllo nell'esercizio delle rispettive funzioni è una componente essenziale del regime europeo di protezione dei dati, non soltanto ai sensi dell'art. 28, par. 1 della direttiva, che prevede l'istituzione di tali autorità[44] ma, come la Corte ha costantemente ritenuto, anche ai termini dell'art. 8, par. 3 della Carta e dell'art. 16, par. 2 TFUE, che assoggettano il rispetto dei diritti delle persone interessate dal trattamento dei dati al controllo di 'autorità indipendenti'[45].

È evidente che le autorità nazionali di controllo non possono pronunciarsi in contrasto con una decisione della Commissione indirizzata agli Stati membri, atto obbligatorio in tutti i suoi elementi e vincolante per tutti gli organi degli Stati che ne sono i destinatari. Tuttavia, e questo è il punto chiave della pronuncia della Corte, una decisione della Commissione *ex* art. 25, par. 6 della direttiva non può eliminare o restringere i poteri espressamente accordati alle autorità nazionali di controllo dall'art. 8, par. 3 della Carta e dall'art. 28 della direttiva, che sono funzionali all'esercizio da parte di tali autorità della competenza relativa alla sorveglianza nell'applicazione delle disposizioni nazionali di attuazione della direttiva.

Elencati in modo indicativo e non esaustivo dall'art. 28, par. 3, tali poteri comprendono innanzitutto il diritto di accedere ai dati oggetto di trattamento e il diritto di raccogliere qualsiasi informazione necessaria all'esercizio della funzione di controllo; in secondo luogo essi comprendo-

[43] Sull'indipendenza delle autorità di controllo la giurisprudenza della Corte di giustizia è costante: v. sentenze 9 marzo 2010, *Commissione c. Germania*, C-518/07, in *Racc.*, 2010, p. I-1885 ss., par. 23; 16 ottobre 2012, *Commissione c. Austria*, C-614/10, ECLI:EU:C:2012:631, par. 36; 8 aprile 2014, *Commissione c. Ungheria*, C-288/12, ECLI:EU:C:2014:237, par. 47.

[44] Cfr. anche il considerando 62 della direttiva stessa, secondo il quale «la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali».

[45] Si noti, tuttavia, che né l'art. 8, par. 3 della Carta, né l'art. 16, par. 2 TFUE affermano che le 'autorità indipendenti' di controllo dei dati debbano essere anche autorità «nazionali». Stando a queste norme, potrebbe benissimo trattarsi di un organo indipendente istituito a livello europeo. In realtà, l'esistenza di autorità 'nazionali' di protezione dei dati non è altro che è il risultato del fatto che l'attuale sistema europeo di protezione dei dati è basato su una direttiva, che è uno strumento che deve essere implementato a livello nazionale dai singoli Stati membri. Pertanto, lo *status* di indipendenza delle autorità presenti a livello nazionale non è coperto dal diritto primario dell'Unione europea, ma soltanto dall'art. 28, par. 1 della direttiva: cfr. G. Thüsing, J. Traut, *The Reform of European Data Protection Law: Harmonisation at Last?*, in *Intereconomics*, 2013, p. 271 ss., a p. 273.

no poteri effettivi di decisione e di intervento, come quello di ordinare il congelamento, la cancellazione e la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento; da ultimo, il potere di promuovere azioni giudiziarie e di agire in giudizio in caso di violazione delle disposizioni nazionali di attuazione della direttiva. Osserva la Corte che l'art. 28, par. 3 non esclude dalla sfera di competenza delle autorità nazionali di controllo la vigilanza sui trasferimenti di dati verso Stati terzi che siano stati oggetto di una decisione di adeguatezza della Commissione[46]. Pertanto, in linea con le conclusioni dell'Avvocato generale[47], la Corte dichiara che il potere di verificare l'adeguatezza del livello di protezione esistente in uno Stato terzo deve ritenersi condiviso dalla Commissione con le autorità nazionali di controllo.

Si noti che la Corte di giustizia abbandona tutti i distinguo che aveva avanzato nella sentenza *Bodil Lindqvist* per circoscrivere i trasferimenti di dati ai quale è applicabile la direttiva da quelli sottratti alle sue garanzie. E si noti anche che il par. 2 dell'art. 25 non indica che la valutazione dell'adeguatezza del livello di protezione garantito da uno Stato terzo debba spettare alle autorità nazionali di controllo. In effetti, come si è visto, la direttiva non specifica a quale soggetto competa la valutazione dell'adeguatezza: l'individuazione di tale soggetto rientra nel margine di discrezionalità degli Stati membri, che possono attribuire tale potere anche al responsabile del trattamento, come è avvenuto in diversi casi.

Ciò non toglie che, se la Commissione ha constatato, a norma della direttiva, che un paese terzo garantisce un livello di protezione adeguato», l'art. 25, par. 6 stabilisce che «gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione». L'obbligo degli Stati membri di applicare la decisione di adeguatezza della Commissione non è altro che una specificazione dell'art. 288 TFUE, come aveva già osservato il *Data Protection Commissioner*. Del resto, anche il principio del primato del diritto dell'Unione europea, sviluppato nella stessa giurisprudenza della Corte di giustizia, induce a escludere che gli organi di uno Stato membro possano adottare atti non conformi a un obbligo contenuto in una valida decisione della Commissione[48].

Da questo punto di vista, lascia perplessi la conclusione della Corte di

[46] V. par. 54 della sentenza.
[47] V. par. 71 e 85 delle conclusioni.
[48] Sull'effetto preclusivo del principio del primato del diritto dell'Unione v., per tutti, A. Arena, *Il principio della* preemption *in diritto dell'Unione europea. Esercizio delle competenze e ricognizione delle antinomie tra diritto derivato e diritto nazionale*, Napoli, 2013, p. 9 ss..

giustizia, secondo la quale le autorità nazionali di controllo hanno l'obbligo di valutare la legittimità del trasferimento dei dati verso un determinato Stato terzo, in 'piena indipendenza' rispetto alla decisione di adeguatezza della Commissione[49]. Ci si può chiedere infatti quale carattere obbligatorio e vincolante residui per la decisione della Commissione, intesa come atto di diritto derivato, se le autorità degli Stati membri possono valutare la situazione esistente nello Stato terzo indipendentemente dal disposto della decisione stessa. Ci si può chiedere, inoltre, se la pronuncia della Corte valga anche per le decisioni di non adeguatezza, che la Commissione può emanare *ex* art. 25, par. 4, e se anche rispetto ad esse i garanti nazionali abbiano un autonomo potere di valutazione. Ci si può chiedere, ancora, se questo autonomo potere di valutazione possa essere esteso anche alle decisioni della Commissione che hanno approvato *binding corporate rules* o *standard contractual clauses*. Potrebbero essere giudicate inadeguate anche le garanzie che hanno giustificato le decisioni della Commissione riferite all'applicazione di queste deroghe nei trasferimenti verso gli Stati Uniti, considerato che, nella fattispecie, non può escludersi una possibile ingerenza delle autorità americane anche sui dati personali trasferiti in forza di tali strumenti?

Infine, ci si può chiedere se, oltre a «verificare, in piena indipendenza, se il trasferimento [dei dati personali] rispetti i requisiti fissati dalla direttiva»[50], le autorità nazionali di controllo possano anche sospendere o vietare, se del caso, i trasferimenti di tali dati verso il Paese terzo che ritengano inadeguato, malgrado l'esistenza di una decisione di adeguatezza della Commissione riferita a quello Stato terzo. L'Avvocato generale ha ritenuto che alle autorità nazionali di controllo spetta, in questo caso, «il potere di sospendere il trasferimento di dati in parola, e ciò a prescindere dalla valutazione generale effettuata dalla Commissione nella sua decisione»[51]. Sembra difficile, tuttavia, giungere a una simile conclusione senza attribuire sostanzialmente una portata extraterritoriale ai poteri delle autorità di controllo, poteri che, per espressa previsione della direttiva, hanno efficacia esclusivamente limitata al territorio dello Stato membro nel quale tali autorità sono state istituite (art. 28, par. 6). La territorialità dei poteri delle autorità nazionali di controllo è stata espressamente riaffermata dalla Corte di giustizia nella sentenza *Weltimmo*, emanata a ridosso della sentenza *Schrems*, che ha escluso che l'autorità di controllo di uno Stato mem-

[49] Par. 58 della sentenza; v. anche la pronuncia della Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland* cit., par. 68.
[50] Par. 57 della sentenza.
[51] Par. 81 delle conclusioni.

bro possa esercitare i «poteri effettivi d'intervento» che le sono attribuiti dalla direttiva sul territorio di un altro Stato membro[52]. Ma se le autorità nazionali di controllo non possono sospendere o vietare i trasferimenti dei dati verso il Paese che ritengano inadeguato, quale effettività ha il potere di valutazione che tali autorità devono esercitare 'in piena indipendenza'?

Stando a quanto si limita ad affermare esplicitamente la Corte, le autorità nazionali di controllo, in presenza di una decisione di adeguatezza della Commissione, hanno l'obbligo di 'esaminare la domanda' di una persona relativamente alla tutela dei suoi diritti con riferimento al trattamento di dati personali che la riguardano. Sembra, quindi, che tali autorità siano tenute soltanto a ricevere i ricorsi individuali *ex* art. 28, par. 4 della direttiva, proposti a seguito di asserite violazioni del diritto alla protezione dei dati personali, verificatesi a seguito di un trasferimento internazionale dei dati. Qualora l'autorità nazionale di controllo respinga il reclamo, l'interessato potrà accedere al ricorso giurisdizionale che gli Stati membri sono obbligati a predisporre avverso le decisioni di rigetto di tale autorità, in conformità all'art. 28, par. 3 della direttiva. In quella sede, l'interessato potrà sollecitare l'autorità giudiziaria ad effettuare un rinvio pregiudiziale di validità alla Corte di giustizia avverso la decisione di adeguatezza della Commissione – rinvio pregiudiziale che, peraltro, rientra esclusivamente nella discrezionalità del giudice adito, e risulta obbligatorio soltanto per gli organi giurisdizionali di ultima istanza, *ex* art. 267 TFUE[53].

Qualora invece l'autorità nazionale di controllo consideri fondato il reclamo che le è stato proposto, e ritenga inadeguato il livello di protezione esistente nello Stato verso il quale sono stati trasferiti i dati, è incerto, sulla base della sentenza *Schrems*, se questa autorità, oltre ad 'esaminare la domanda', possa anche accogliere il ricorso ed emettere i conseguenti provvedimenti, provvisori o definitivi, relativi alla sua esecuzione. Infatti, la Corte si limita a dichiarare che, qualora ritenga fondato il reclamo, l'autorità nazionale di controllo dovrà adire l'autorità giudiziaria, *ex* art. 28, par. 3 della direttiva, sollecitando un rinvio pregiudiziale sulla validità della decisione della Commissione.

[52] In questo caso, l'autorità in questione dovrà limitarsi a chiedere l'intervento dell'autorità di controllo dello Stato membro sul territorio del quale dovrebbe aver luogo l'esecuzione: cfr. Corte di giustizia, 1° ottobre 2015, causa C 230/14, *Weltimmo* cit., par. 60.

[53] Giurisprudenza costante: cfr., ad es., Corte di giustizia, 7 dicembre 2010, *VEBIC VZW*, causa C-439/08, in *Racc.*, 2010, p. I-12471 ss., par. 41; Corte di giustizia, 2 aprile 2009, *Pedro IV Servicios*, causa C260/07, *ibid.*, p. I-2437 ss., par. 28; 14 dicembre 2006, *Confederación Española de Empresarios de Estaciones de Servicio*, causa C 217/05, *ibid.*, 2006, p. I-11987 ss., par. 16.

La Corte sembra implicitamente escludere che le autorità nazionali di controllo dei dati possano proporre autonomamente il rinvio pregiudiziale alla Corte di giustizia. Si potrebbe sostenere che tali autorità non presentino i requisiti di «*organi giurisdizionali* degli Stati membri» che, a norma dell'art. 267 TFUE, devono obbligatoriamente riscontrarsi nell'autorità remittente[54]. Tuttavia, l'accento posto dalla Corte di giustizia sulla 'completa indipendenza' di tali autorità, l'aver attribuito loro l'obbligo di tutelare diritti fondamentali della persona, il fatto che esse esercitino una funzione contenziosa in senso stretto, destinata a risolversi in una pronuncia di carattere giurisdizionale, pone seriamente la questione della legittimazione delle autorità nazionali di controllo dei dati a sollevare il rinvio pregiudiziale, anche in vista del fatto che il nuovo regolamento, come si vedrà, aumenterà i poteri e l'indipendenza delle *authorities*.

Nella sentenza *Schrems*, inoltre, la Corte di giustizia interpreta la nozione di 'adeguatezza'. In proposito, la Corte limita innanzitutto la discrezionalità della quale può disporre la Commissione nel valutare questo requisito, tenuto conto, da un lato, del carattere fondamentale del diritto alla protezione dei dati personali e, dall'altro, dell'elevato numero di persone i cui diritti sarebbero a rischio se i loro dati fossero trasferiti verso Paesi dal livello di protezione inadeguato[55]. In secondo luogo, malgrado la direttiva non imponga alla Commissione un obbligo di revisione periodica delle sue decisioni di adeguatezza,[56], la Corte afferma esplicitamente che la

[54] Per costante giurisprudenza, la Corte di giustizia accerta la qualità di «organo giurisdizionale di uno Stato membro», *ex* art. 267 TFUE, che costituisce una nozione autonoma di diritto dell'Unione, verificando l'esistenza, presso l'organo remittente, di una serie di elementi, quali l'origine legale dell'organo, il suo carattere permanente, l'obbligatorietà della sua giurisdizione, la natura contraddittoria del procedimento, il fatto che l'organo applichi norme giuridiche e che sia indipendente: cfr., ad es., Corte di giustizia, 17 settembre 1997, causa C-54/96, *Dorsch Consult*, in *Racc.*, 1997, p. I-4961 ss., par. 23; 30 novembre 2000, causa C-195/98, Österreichischer Gewerkschaftsbund, *ibid.*, p. I-10497 ss., par. 24; 30 maggio 2002, causa C-516/99, *Schmid*, *ibid.*, 2002, p. I-4573 ss., par. 34; 22 dicembre 2010, *Koller*, causa C-118/09, *ibid.*, 2010, p. I-13627 ss., par. 22 s.; 22 dicembre 2010; *RTL Belgium*, causa C-517/09, *ibid.*, p. I-14093 ss., par. 36 ss.; 14 giugno 2011, *Miles et al.*, causa C-196/09, *ibid.*, 2011, p. I-5105 ss., par. 37 ss. Inoltre, i giudici nazionali possono adire la Corte soltanto se dinanzi ad essi sia pendente un procedimento destinato a risolversi in una pronuncia di carattere giurisdizionale: v. Corte di giustizia, 19 ottobre 1995, *Job Centre*, causa C-111/94, in *Racc.*, 1995, p. I-3361, par. 9; 31 maggio 2005, C-53/03, *Syfait*, *ibid.*, 2005, p. I-4609 ss., par. 29.

[55] In questo senso v. anche la sentenza della Corte di giustizia dell'8 aprile 2014, *Digital Rights Ireland* cit., par. 48.

[56] E malgrado la decisione relativa al «*Safe Harbor*» impegnasse la Commissione ad un'unica valutazione della sua applicazione, tre anni dopo l'entrata in vigore: cfr. art. 4 della

Commissione è tenuta a verificare periodicamente che l'adeguato livello di protezione garantito dallo Stato terzo si mantenga giustificato nel tempo, da un punto di vista fattuale e legale[57]. La Corte accolla alla Commissione un vero e proprio obbligo: può quindi ritenersi che, qualora questa istituzione ometta di adempiervi, in presenza di circostanze sopravvenute che giustifichino dubbi sulla persistenza delle garanzie assicurate dallo Stato terzo, si possa prospettare la proposizione di un ricorso in carenza avverso la Commissione, *ex* art. 265 TFUE.

Per quanto riguarda il merito della definizione di 'adeguatezza', la Corte riconosce innanzitutto che 'adeguato' non significa 'identico', secondo quanto già evidenziato dal Gruppo Art. 29. È ammissibile, quindi, secondo la Corte, che il livello di protezione assicurato dal Paese terzo presenti delle differenze rispetto a quello garantito nel diritto dell'Unione europea. Lo Stato terzo, tuttavia, deve assicurare 'effettivamente' ai diritti della persona interessata una tutela 'sostanzialmente equivalente' a quella garantita nell'ordinamento dell'Unione dalla direttiva e dalla Carta dei diritti fondamentali[58]. Inutile sottolineare quanto questa richiesta da parte della Corte appaia intrinsecamente contraddittoria: una protezione 'effettiva' ed 'equivalente' a quella assicurata dall'Unione europea non è altro, infatti, che una protezione sostanzialmente identica a quella esistente nell'Unione europea. L'espressione adoperata dalla Corte ricorda da vicino l'endiadi dell'«effettività ed equivalenza di tutela», da tempo utilizzata dalla Corte di giustizia per limitare l'autonomia procedurale *degli Stati membri* nella predisposizione della tutela di diritti spettanti ai singoli in forza del diritto dell'Unione[59]. In questa sentenza, tuttavia, questi principi sono applicati dalla Corte *nei confronti di Stati terzi rispetto all'Unione*. Se la premessa della motivazione della Corte è analoga a quello del Gruppo Art. 29, le conclusioni non potrebbero essere più distanti.

In applicazione di questo rigoroso *test* di effettività ed equivalenza, la Corte prende dunque in esame la decisione della Commissione relativa al «Safe Harbor» e osserva, innanzitutto, che questo atto non certifica l'adeguatezza del livello di protezione dei dati relativo all'ordinamento degli Stati Uniti complessivamente considerato, ma soltanto quella del sistema istituito dall'accordo negoziato dalla Commissione. Il «Safe Harbor» infatti è applicabile soltanto alle imprese e alle organizzazioni che

decisione.

[57] Par. 76 della sentenza.

[58] Par. 73-74 della sentenza.

[59] Giurisprudenza consolidata: v. già Corte di giustizia, 16 dicembre 1976, *Rewe*, causa 33/76, in *Racc.*, 1976, p. 1989 ss.; 16 dicembre 1976, *Comet*, causa 45/76, *ibid.*, 2043 ss.

vi abbiano specificamente aderito, ma non vincola le autorità pubbliche e le istituzioni americane, che non risultano tenute ad osservarne i principi.

La Corte riscontra, in secondo luogo, che il «Safe Harbor» è carente relativamente all'effettività delle misure e delle procedure di vigilanza, peraltro particolarmente necessarie per un sistema del genere, sostanzialmente basato sull'autocertificazione di un impegno volontariamente assunto dai partecipanti.

In terzo luogo, questo accordo, come si è visto, non soltanto consente alle autorità statunitensi di derogare ai principi di legittimità del trattamento, e quindi di accedere ai dati per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia[60], ma permette altresì agli aderenti di sottrarsi legittimamente alla sua applicazione, in presenza di atti legislativi, amministrativi o giurisprudenziali che li obblighino o li autorizzino a disapplicare l'accordo per finalità di tutela dell'interesse pubblico[61].

Infine, secondo la Corte, il «Safe Harbor» non predispone sufficienti presidi giuridici per limitare questa ingerenza, né prevede concreti controlli amministrativi o rimedi giurisdizionali per le persone interessate che siano cittadine europee o residenti negli Stati membri dell'Unione, qualora i loro dati personali siano stati oggetto, da parte delle autorità americane, di accessi illegittimi, determinando così una disparità di trattamento rispetto ai cittadini americani. La Corte ricorda anche che tutte queste insufficienze, già evidenziate a suo tempo dal Gruppo Art. 29[62], possono considerarsi dimostrate, poiché sono state esplicitamente ammesse dalla stessa Commissione, che ha riconosciuto che il «Safe Harbor» non ha di fatto salvaguardato i dati personali dei cittadini europei dagli accessi ingiustificati effettuati delle autorità degli Stati Uniti[63].

Tali restrizioni sono illegittime, secondo la Corte, non perché un diritto fondamentale, qual è quello alla protezione dei dati personali, non

[60] Cfr. all. I alla decisione cit., par. 4, lett. a).
[61] Cfr. all. I alla decisione cit., par. 4, lett. b).
[62] V., in proposito, WP29, *Opinion 7/99 On the Level of Data Protection Provided by the «Safe Harbor» Principles as Published Together with the Frequently Asked Questions (FAQs) and Other Related Documents on 15 and 16 November 1999 by the US Department of Commerce*, WP 27/99 del 3 dicembre 1999, spec. p. 11 ss.; Id., *Opinion 1/99 Concerning the Level of Data Protection in the United States And the Ongoing Discussions Between the European Commission and the United States Government*, WP15/99 del 26 gennaio 1999, p. 2-4.
[63] V. la comunicazione della Commissione «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» cit., par. 2 e 3.2; e la relazione della Commissione stessa sul «Funzionamento del regime *'Approdo sicuro'*» cit., par. 7 e 8.

possa ammettere limitazioni giustificate da esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia. Lo stesso art. 8, par. 2 CEDU, sulla base del quale deve essere interpretato il diritto alla protezione dei dati personali contenuto nell'art. 8 della Carta, ammette che possano esservi ingerenze dell'autorità pubblica nell'esercizio del diritto alla riservatezza, a condizione che ciascuna di esse sia prevista dalla legge e costituisca «una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui». Tuttavia, la Corte, richiamando la sua giurisprudenza nel caso *Digital Rights Ireland*[64], afferma che tali restrizioni devono essere contenute «entro i limiti dello stretto necessario». E i principi di necessità e di proporzionalità risultano violati quando l'autorità pubblica può effettuare accessi indiscriminati e generalizzati al contenuto dei dati, «senza alcuna differenziazione, limitazione o eccezione in funzione degli obiettivi perseguiti».[65] Una simile ingerenza viola il diritto fondamentale al rispetto della vita privata e alla riservatezza dei dati personali, nonché il diritto ad un effettivo rimedio giurisdizionale, *ex* art. 7, 8 e 47 della Carta. Su questa base, la Corte dichiara quindi invalido l'art. 1 della decisione della Commissione relativa al «Safe Harbor».

[64] Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland* cit., par. 32-37 e 65 della sentenza. La sentenza aveva dichiarato invalida la direttiva 2006/24/CE riguardante la conservazione di dati nei servizi di comunicazione elettronica accessibili al pubblico e nelle reti pubbliche di comunicazione. La direttiva, in particolare, obbligava i fornitori di questi servizi a conservare per un certo periodo i metadati relativi al traffico, all'ubicazione e ad altre informazioni, che possono consentire l'identificazione dell'abbonato o dell'utente; inoltre, permetteva l'accesso delle autorità nazionali al contenuto dei dati, senza che vi fosse obbligo di informare la persona interessata; infine, non imponeva che i dati fossero conservati sul territorio degli Stati membri e pertanto non garantiva, secondo la prospettiva allora espressa dalla Corte, il pieno controllo da parte delle autorità indipendenti del rispetto delle esigenze di protezione e di sicurezza, che è stato esplicitamente richiesto dall'articolo 8, par. 3, della Carta quale elemento essenziale della protezione dei diritti delle persone relativi al trattamento dei dati personali. La Corte aveva concluso che tutte queste carenze costituivano un'ingerenza grave nel diritto fondamentale alla protezione dei dati di carattere personale, sancito dall'art. 7 e dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea. Trattandosi di ingerenza non proporzionata, né limitata allo stretto necessario, così seria da violare la sostanza stessa del diritto fondamentale alla tutela dei dati personali, la Corte aveva quindi annullato la direttiva. V. anche le conclusioni dell'Avv. gen. Cruz Villalón del 12 dicembre 2013, ECLI:EU:C:2013:845, in particolare par. 39-40, 77, 80.

[65] Par. 93 della sentenza.

La Corte dichiara invalido anche l'art. 3 di tale decisione. Come si è visto, questa norma consente alle autorità nazionali di controllo di sospendere i trasferimenti di dati diretti verso un'impresa o un'organizzazione aderente al «Safe Harbor», qualora siano stati violati i principi di legittimità del trattamento, applicati in conformità agli orientamenti applicativi contenuti nella decisione, o qualora «sia molto probabile che i principi vengano violati», senza che venga posto effettivo rimedio a questo inadempimento. Tuttavia, le condizioni richieste per l'applicazione dell'art. 3 sono così restrittive, da convincere la Corte che questa disposizione in realtà sottrae alle autorità nazionali di controllo una parte dei poteri di intervento che sono stati loro attribuiti dall'art. 28 della direttiva. Poiché tuttavia la Commissione non poteva restringere i poteri conferiti dalla direttiva alle autorità di controllo, la Corte dichiara l'invalidità anche dell'art. 3 della decisione. Infine, considerata l'inseparabilità dell'art. 1 e dell'art. 3 dal resto dell'atto, dichiara invalida tutta la decisione relativa al «Safe Harbor»[66].

Gli effetti dell'invalidità retroagiscono al momento nel quale la decisione della Commissione è entrata in vigore[67]. Infatti, la Corte sceglie di non avvalersi della facoltà di limitare nel tempo gli effetti della sentenza, esponendo consapevolmente gli operatori alle gravi ripercussioni economiche causate dall'invalidità retroattiva del «Safe Harbor». La retroattività della dichiarazione di invalidità appare come un'arma della quale la Corte si serve per costringere la Commissione ad accelerare la rinegoziazione del «Safe Harbor». Al momento della pronuncia della sentenza *Schrems*, infatti, la conclusione delle trattative con gli Stati Uniti appariva ancora lontana, benché i negoziati fossero stati avviati prima della proposizione del rinvio pregiudiziale alla Corte di giustizia. Alle pressioni da parte della Corte si sono aggiunte, all'indomani della sentenza *Schrems*, quelle del

[66] Si noti che la decisione relativa al «*Safe Harbor*» non avrebbe potuto essere oggetto di un autonomo ricorso dinanzi alla Corte di giustizia per annullamento ex art. 263 TFUE, considerato che il termine perentorio di proposizione del ricorso è di due mesi a decorrere dalla pubblicazione dell'atto nella Gazzetta Ufficiale dell'Unione europea, o dalla notificazione al destinatario, oppure, in mancanza di pubblicazione o di notifica, dal momento in cui il ricorrente è venuto a conoscenza dell'atto stesso: cfr. art. 263 TFUE, ult. comma.

[67] Talvolta, la Corte di giustizia, al fine di evitare che la retroattività di principio delle sentenze dichiarative dell'invalidità (risalente al momento in cui l'atto è entrato in vigore) possa pregiudicare diritti acquisiti in buona fede, ha attribuito alle proprie decisioni di annullamento, in via di eccezione e sulla base del principio generale del legittimo affidamento e della certezza del diritto, un effetto ex nunc. Sulla possibilità di limitare nel tempo gli effetti delle sentenze dichiarative dell'invalidità degli atti cfr. già Corte di giustizia, 8 aprile 1976, causa 43/75, *Defrenne II*, in *Racc.*, 1976, p. 455.

Gruppo Art. 29, che ha dichiarato che le autorità garanti nazionali non avrebbero escluso 'azioni coordinate', nel caso in cui la Commissione, entro la fine di gennaio 2016, non avesse trovato 'un'appropriata soluzione' con il governo degli Stati Uniti per rimediare al vuoto normativo creatosi con l'invalidità del «Safe Harbor»[68].

Prendendo atto dell'orientamento della Corte di giustizia e dell'avvertimento, neanche troppo velato, proveniente dal Gruppo Art. 29, la Commissione ha accelerato le trattative per sostituire il «Safe Harbor» – pur rammentando agli operatori che, nel frattempo, avrebbero potuto proseguire i trasferimenti oltreoceano dei dati utilizzando le deroghe previste dall'art. 26 della direttiva, sia pure con l'obbligo di richiedere le relative autorizzazioni caso per caso[69]. Tuttavia, come subito precisato dal Gruppo Art. 29, i trasferimenti in deroga non offrono alcuna protezione contro l'accesso ai dati da parte dell'autorità pubblica per ragioni di sicurezza nazionale[70].

4. La proposta relativa a una nuova decisione di adeguatezza della Commissione: il «Privacy Shield»

Il 29 febbraio 2016 la Commissione ha annunciato di aver finalmente raggiunto l'intesa con gli Stati Uniti sul nuovo quadro giuridico per lo scambio di dati destinato a sostituire il «Safe Harbor»[71] e ha presentato, con una sua comunicazione, la proposta relativa alla decisione di adeguatezza dell'«EU-US Privacy Shield» (o «Scudo per la riservatezza»). Così come nel caso del «Safe Harbor», anche in questo caso oggetto di valu-

[68] Cfr. «Statement of the Article 29 Working Party» del 16 ottobre 2015: «If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions.»

[69] Si veda la comunicazione della Commissione al Parlamento europeo e al Consiglio relativa al trasferimento di dati personali dall'UE agli Stati Uniti, in applicazione della direttiva 95/46/CE a seguito della sentenza della Corte di giustizia nella causa C-362/14, (*Schrems*), COM(2015)566 def. del 6 novembre 2015, p. 6 ss.

[70] Cfr. «*Statement of the Article 29 Working Party*» cit., e l'analogo «*Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment*» del 3 febbraio 2016.

[71] Cfr. comunicazione della Commissione al Parlamento europeo e al Consiglio *Trasferimenti transatlantici di dati – Ripristinare la fiducia attraverso solide garanzie* (COM(2016)117 def. del 29 febbraio 2016, spec. p. 8 ss.

tazione non è il complesso dell'ordinamento giuridico degli Stati Uniti, ma soltanto lo specifico sistema di protezione istituito appositamente dal governo americano per il trattamento dei dati trasferiti a partire dall'Unione europea. Questo comprende un elenco di principi che le organizzazioni aderenti saranno tenute a rispettare nell'ambito dell'accordo, l'istituzione di specifici organismi tenuti a vigilare sul rispetto di tali principi, e la predisposizione di una serie di mezzi di ricorso individuale per l'applicazione di sanzioni in caso di violazione dell'accordo. Tuttavia, con una significativa novità rispetto al «Safe Harbor», il governo degli Stati Uniti rilascerà impegni scritti e dichiarazioni ufficiali sull'applicazione dell'accordo che, a conferma della loro vincolatività, saranno pubblicati nell'*U.S. Federal Register*.

I pilastri del «Privacy Shield» sono rappresentati, innanzitutto, dall'imposizione alle organizzazioni aderenti di precisi obblighi giuridicamente vincolanti, e non più soltanto volontariamente assunti. Tali organizzazioni risulteranno responsabili anche qualora trasferiscano dati di cittadini dell'Unione a soggetti terzi, esterni all'accordo, che si trovino negli Stati Uniti o in Paesi terzi (c.d. 'trasferimenti successivi', ad esempio per attività di trattamento dei dati in subfornitura).

In secondo luogo, le autorità governative degli Stati Uniti rilasceranno specifiche garanzie in relazione alle condizioni per l'accesso ai dati effettuato ai fini di amministrazione della giustizia, di sicurezza nazionale e per altri scopi di interesse pubblico. Tali garanzie riguarderanno sia l'apposizione di precisi limiti all'accesso da parte delle autorità pubbliche di sicurezza (verrà impedito, tra l'altro, l'accesso indiscriminato ai dati), sia l'azionabilità dei diritti individuali sanciti dall'ordinamento americano sulla tutela della vita privata, in particolare attraverso l'estensione ai cittadini dell'Unione europea di alcuni diritti di ricorso giudiziario finora esercitabili soltanto dai cittadini statunitensi e dai residenti permanenti. All'interno dell'*US Department of State* verrà inoltre istituito un mediatore indipendente, che avrà l'incarico di trattare i ricorsi di cittadini dell'Unione relativamente all'accesso effettuato per motivi di sicurezza nazionale da parte dell'autorità pubblica. La competenza del mediatore dovrebbe estendersi, in linea di principio, a tutti i dati personali trasferiti negli Stati Uniti per fini commerciali, e non soltanto a quelli trasferiti nel quadro del «Privacy Shield».

Terzo, sarà garantita l'effettività della protezione dei diritti dei cittadini dell'Unione europea attraverso l'istituzione di organismi di vigilanza, con il potere di infliggere sanzioni, che potranno arrivare fino all'esclusione

dei soggetti inadempienti dall'applicazione del «Privacy Shield». Verranno inoltre istituiti mezzi di ricorso individuale, accessibili e di costo sostenibile, tra i quali, in particolare, alcuni organi di risoluzione alternativa delle controversie, e un comitato, che appare come una forma di arbitrato, la cui decisione in ultima istanza sarà vincolante ed esecutiva nei confronti degli operatori aderenti al sistema. Alle organizzazioni americane che trattano dati di cittadini europei relativi alle risorse umane sarà inoltre imposto il rispetto delle decisioni delle autorità garanti europee.

Infine, il «Privacy Shield» prevede un meccanismo annuale di riesame congiunto, che consentirà alla Commissione di monitorare il funzionamento dell'accordo, insieme con il *Department of Commerce* degli Stati Uniti, per verificare che le garanzie in materia di protezione dei diritti individuali fornite al momento del trasferimento dei dati restino equivalenti a quelle in forza nell'Unione europea. Qualora gli operatori economici o le autorità pubbliche americane non tengano fede agli impegni assunti, la Commissione potrà avviare la procedura per la sospensione dell'accordo. La Commissione sarà tenuta a presentare annualmente una relazione al Parlamento europeo e al Consiglio basata sui risultati di tale riesame congiunto.

L'*iter* previsto per l'approvazione della proposta relativa al «Privacy Shield» ha già subito tuttavia una battuta d'arresto, a seguito del parere non del tutto positivo del Gruppo Art. 29, che renderà necessarie sostanziali modifiche al contenuto della decisione.

Il Gruppo ha ravvisato infatti una mancanza di chiarezza e di trasparenza del testo, che lo rende di difficile consultazione, dispersivo, e talvolta incoerente. In particolare, alcune definizioni relative ai principi chiave della *privacy* non combaciano con quelle già adottate negli atti dell'Unione in materia, rischiando di rendere inutilmente complicata l'interpretazione e la futura applicazione di questo strumento.

Il Gruppo Art. 29 sottolinea inoltre che l'accordo, che è stato stilato in riferimento alla direttiva, dovrà esser armonizzato con il nuovo regolamento, e in generale con tutto il pacchetto di riforma dei dati personali che sta per essere emanato. Questo implica la necessità di una revisione a breve dell'accordo; in caso contrario, il Gruppo ritiene che il «Privacy Shield» potrebbe non rispondere al requisito di fornire una protezione 'essenzialmente equivalente', considerato che la riforma garantirà un livello di tutela dei diritti e delle libertà individuali più elevato rispetto alla direttiva. Ad esempio, il Gruppo Art. 29 osserva che il fondamentale diritto relativo alla cancellazione dei dati non è espressamente menzionato nel

testo dell'accordo, e non può essere inferito senza incertezze dal principio relativo all'integrità dei dati e alla limitazione dello scopo della raccolta, poiché quest'ultimo non obbliga i soggetti aderenti alla rimozione dei dati, nel caso in cui la conservazione non risulti più necessaria.

Inoltre, i limiti posti dal «Privacy Shield» all'azione delle autorità pubbliche statunitensi restano suscettibili di essere interpretati con eccessiva discrezionalità. In particolare, il Gruppo Art. 29 ritene che l'allegato VI al «Privacy Shield» non consenta di escludere del tutto che l'autorità governativa degli Stati Uniti possa continuare l'accesso indiscriminato su vasta scala ai dati personali trasferiti dall'Unione europea, in evidente contasto con la pronuncia della Corte di giustizia.

Un ulteriore aspetto riguarda il meccanismo di reclamo che dovrebbe far capo alla figura del mediatore. Benché debba senz'altro essere approvata l'istituzione di un'istanza di ricorso indipendente, in vista di un effettivo esercizio dei diritti individuali, il Gruppo Art. 29 osserva che la figura descritta nell'accordo non sembra esser dotata di poteri sufficienti per vigilare efficacemente e impedire eventuali abusi, anche in considerazione del rinnovato impulso politico alla sorveglianza di massa causato dal timore nei confronti del terrorismo. Inoltre, possono esprimersi legittimi dubbi sull'effettiva terzietà e indipendenza di tale autorità (incardinata all'interno dell'*US Department of State*, come si è visto). Gli altri rimedi previsti dall'accordo sembrano a loro volta troppo complessi per poter essere azionati dai singoli senza eccessive difficoltà, inducendo così a dubitare della loro effettività.

Ancora, poiché il «Privacy Shield» è suscettibile di essere utilizzato per trasferire i dati anche in Paesi terzi rispetto agli Stati Uniti, il Gruppo Art. 29 insiste affinché i trasferimenti esterni rispondano agli stessi requisiti di protezione dei dati personali stabiliti per i trattamenti effettuati nei Paesi oggetto dell'accordo, poiché, in caso contrario, questo genere di trasferimento extraterritoriale rischia di costituire un mezzo per aggirare i principi relativi alla protezione dei dati dell'Unione europea.

Infine, il meccanismo annuale di revisione congiunta, che a parere del Gruppo Art. 29 costituisce un fattore chiave per la credibilità complessiva del «Privacy Shield», soffre di scarsa chiarezza relativamente alle sue modalità di svolgimento, sotto l'aspetto della pubblicità da riservare alla relazione conclusiva dell'esame, delle possibili conseguenze in caso di risultato negativo, e della mancata indicazione dei mezzi di finanziamento. Il Gruppo Art. 29 ritiene inoltre che la revisione dell'accordo dovrebbe coinvolgere anche rappresentanti delle autorità garanti nazionali.

Considerata la gravità dei rilievi mossi dal Gruppo Art. 29, dei quali la Commissione non può non tenere conto, il testo della proposta appare quindi ancora lontano dall'essere definitivo.

Nel frattempo, però, è stato posto un altro tassello per la tutela dei dati dei cittadini europei nei confronti delle autorità americane. Infatti, l'8 settembre 2015, dopo quattro anni di trattative, iniziate quasi in parallelo all'avvio della riforma della direttiva, è stato firmato un accordo quadro tra l'Unione europea e gli Stati Uniti per la protezione dei dati personali in materia penale[72]. L'accordo, chiamato «the Umbrella Agreement» si propone di di assicurare un elevato grado di protezione dei dati personali – prevalentemente giudiziari e comunque pertinenti a tali finalità – scambiati tra magistratura, autorità giudiziarie e organismi di polizia, nel quadro della cooperazione transatlantica per la lotta al terrorismo e alla criminalità organizzata.

5. I trasferimenti dei dati verso Stati terzi, le decisioni di adeguatezza della Commissione e i poteri delle autorità nazionali di controllo nel nuovo regolamento generale sulla protezione dei dati personali

Lo scenario di riferimento, per quanto riguarda la protezione dei dati personali nell'Unione europea, è destinato a cambiare a breve. Infatti, il nuovo regolamento generale di protezione dei dati, che dovrà sostituire la direttiva, sta per concludere l'*iter* relativo alla sua approvazione definitiva. L'insistenza da parte della sentenza *Schrems* su determinati argomenti sembra spiegarsi proprio con la volontà della Corte di giustizia di incidere su alcuni aspetti del nuovo regolamento che possono ancora essere modificati.

Per quanto riguarda specificamente i trasferimenti dei dati verso Stati terzi, il nuovo regolamento, nel testo provvisorio attualmente disponibile,[73] ricalca nelle sue linee fondamentali la struttura prevista dalla direttiva:

[72] *Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses*, in http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf. La decisione di attuazione dell'accordo verrà adottata dal Consiglio dopo l'approvazione del Parlamento europeo.

[73] Il testo provvisoriamente disponibile consolida gli emendamenti apposti dal Parlamento europeo in prima lettura: cfr. risoluzione legislativa del Parlamento europeo del 12 marzo 2014 sulla proposta di regolamento del Parlamento europeo e del Consiglio concernente

il principio generale è ancora quello dell'autorizzazione condizionata alla verifica della conformità del trasferimento ai principi di legittimità del trattamento (art. 40). Ancora una volta, il trasferimento non richiede una specifica autorizzazione, qualora la Commissione decida con un atto delegato – previa acquisizione del parere obbligatorio, ma non vincolante, del Comitato europeo per la protezione dei dati – che lo Stato terzo, o l'organizzazione internazionale ove il trasferimento è diretto, assicuri un adeguato livello di protezione (art. 41).[74] Tuttavia, a differenza della direttiva, il nuovo regolamento precisa nel dettaglio una lunga lista di elementi che la Commissione è tenuta a prendere in considerazione per verificare l'adeguatezza[75], restringendo quindi la sua discrezionalità nell'effettuare tale valutazione, così come richiesto dalla Corte di giustizia nella sentenza *Schrems*.

È anche possibile identificare una traccia dell'approccio funzionale proposto dal Gruppo Art. 29 nella sezione del regolamento che prevede che, per verificare l'adeguatezza del livello di protezione dei dati, il

la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), P7_TA(2014)0212.

[74] Art. 41, par. 1 e 3 del testo provvisorio del regolamento: «1. Il trasferimento è ammesso se la Commissione ha deciso che il paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche. […] 3. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'art. 86, al fine di decidere che un paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o un'organizzazione internazionale garantisce un livello di protezione adeguato ai sensi del par. 2. […]».

[75] Art. 41, par. 2, del testo provvisorio del regolamento: «2. Nel valutare l'adeguatezza del livello di protezione la Commissione prende in considerazione i seguenti elementi: *a)* lo stato di diritto, la pertinente legislazione generale e settoriale vigente, anche in materia penale, di pubblica sicurezza, difesa e sicurezza nazionale, come anche l'attuazione di tale legislazione, le regole professionali e le misure di sicurezza osservate nel paese terzo o dall' organizzazione internazionale in questione, la giurisprudenza precedente nonché i diritti effettivi e azionabili, compreso il diritto degli interessati a un ricorso effettivo in sede amministrativa e giudiziaria, in particolare quelli che risiedono nell' Unione e i cui dati personali sono oggetto di trasferimento; *b)* l' esistenza e l' effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o nell' organizzazione internazionale in questione, incaricate di garantire il rispetto delle norme di protezione dei dati, anche con sufficienti poteri sanzionatori, assistere e consigliare gli interessati in merito all' esercizio dei loro diritti e cooperare con le autorità di controllo dell' Unione e degli Stati membri, e *c)* gli impegni internazionali assunti dal paese terzo o dall' organizzazione internazionale in questione, in particolare ogni convenzione o strumento giuridicamente vincolante in relazione alla protezione dei dati personali».

responsabile del trattamento – o, se del caso, l'incaricato – avrà l'obbligo di effettuare un'analisi preventiva dei rischi generati dal trattamento sui diritti e sulle libertà della persona interessata, nonché una valutazione di impatto e una revisione di conformità delle procedure adoperate nel trattamento stesso, prendendo in esame tutte le circostanze concrete, con specifica attenzione all'effettività della situazione, ed evitando qualsiasi valutazione aprioristica (art. 32 *bis* ss.).

Il regolamento riflette le richieste della Corte di giustizia anche sotto l'aspetto dell'obbligo, esplicitamente accollato alla Commissione, di monitorare continuativamente gli sviluppi della situazione esistente nello Stato terzo (o nell'organizzazione internazionale) ove sono stati trasferiti i dati, allo scopo di individuare eventuali cambiamenti nelle circostanze che potrebbero giustificare modifiche alla decisione di adeguatezza[76]. In particolare, qualora nel Paese terzo non dovesse più riscontrarsi il livello di protezione inizialmente esistente nella tutela dei diritti delle persone residenti nell'Unione, la Commissione avrà l'obbligo di revocare la decisione di adeguatezza, e potrà anche adottare una decisione di non adeguatezza, attraverso atti delegati o di esecuzione[77].

In mancanza di una decisione di adeguatezza della Commissione, o qualora vi sia una decisione di non adeguatezza, il regolamento riconferma, in continuità con la direttiva, il divieto di trasferire dati personali verso lo Stato o l'organizzazione internazionale che siano stati ritenuti inadeguati (art. 42, par. 1).

Ancora una volta, tuttavia, il divieto cade, e il responsabile o l'incaricato del trattamento può trasferire dati verso uno Stato terzo (o verso un'organizzazione internazionale) senza dover essere specificamente autorizzato, a condizione che offra garanzie adeguate contenute in uno strumento giuridicamente vincolante che sia stato approvato dall'autorità

[76] Cfr. art. 41, par. 3, *in fine* e, rispettivamente, par. 4 *bis* del testo provvisorio del regolamento: «3. […] Tali atti delegati prevedono una clausola di estinzione se riguardano un settore di trattamento e sono revocati a norma del par. 5 qualora non sia più garantito un livello adeguato di protezione in conformità del presente regolamento. […] 4 *bis*. La Commissione controlla, su base continuativa, gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sugli elementi di cui al par. 2 [v. nota precedente] qualora sia stato adottato un atto delegato ai sensi del par 3 [v. *supra*, nota 74]».

[77] Art. 41, par. 5 del testo provvisorio del regolamento. La Commissione sarà obbligata inoltre a rivedere tutte le decisioni di adeguatezza adottate dalla Commissione sulla base della direttiva. Queste resteranno in forza soltanto per cinque anni dopo l'entrata in vigore del regolamento, se non modificate, sostituite o abrogate prima dalla Commissione: v. art. 41, par. 8 del testo provvisorio del regolamento.

nazionale di controllo[78]. Questi strumenti, elencati in via esemplificativa e non esaustiva dall'art. 42, par. 2 del regolamento, sono ancora costituiti dalle norme vincolanti d'impresa; le clausole *standard* di protezione dei dati, che siano state dichiarate di validità generale dalla Commissione[79]; le clausole contrattuali tra il responsabile o l'incaricato del trattamento e il destinatario dei dati; e infine, con una novità introdotta dal regolamento, il «sigillo europeo di protezione dei dati» (art. 39, par. 1, lett. *aa*). Questo costituisce una sorta di marchio di conformità, un contrassegno concesso dall'autorità nazionale di controllo a conclusione di una procedura amministrativa volta a certificare che il trasferimento dei dati è effettuato in conformità con le norme del regolamento, allo scopo di segnalare al pubblico l'adozione volontaria, da parte del responsabile o dell'incaricato del trattamento, di una serie di misure, procedure e controlli a garanzia della legittimità del trasferimento.

Non è stata invece ricompresa, tra gli strumenti giuridicamente vincolanti, una *best practice* che, con l'avallo del Gruppo Art. 29, inizia a svilupparsi a livello interno, costituita dalla certificazione indipendente effettuata da un ente di standardizzazione, che verifichi, da una prospettiva di terzietà, la conformità del trattamento agli obblighi e agli adempimenti posti a carico del responsabile del trattamento[80].

Anche il nuovo regolamento prevede, in via di eccezione, la possibilità di derogare al divieto di trasferire dati verso uno Stato terzo o un'organizzazione internazionale che non garantiscano un livello adguato di protezione (o che non siano stati oggetto di una decisione di adeguatezza della Commissione).

Le deroghe, previste dall'art. 44 del regolamento, sono sostanzialmente le stesse consentite dalla direttiva: il consenso informato e specifico della persona interessata; la necessità di concludere o eseguire un contratto tra la persona interessata e il responsabile del trattamento, oppure tra questi e

[78] Se del caso, in conformità al meccanismo di coerenza di cui all'art. 57 del regolamento: v. *infra* nel testo.

[79] Cfr. art. 62, par. 1, lett. *b* del testo provvisorio del regolamento. Le clausole contrattuali approvate dall'autorità di controllo sulla base dell'art. 26, par. 2 della direttiva resteranno valide per due anni dopo l'entrata in vigore del nuovo regolamento, se non modificate, sostituite o abrogate dall'autorità entro questo periodo di tempo: art. 42, par. 5 del testo provvisorio del regolamento.

[80] Cfr., ad es., la norma ISO 27018 per *public cloud*, pubblicata nel 2014 dall'ente di certificazione internazionale ISO quale standard specifico per garantire il rispetto della direttiva 95/46/CE da parte di *providers* che gestiscono infrastrutture informatiche distribuite seguendo il modello del *cloud* pubblico (benché l'adozione di contratti e accordi vincolanti non sia obbligatoria, ma lasciata alla discrezionalità del *service provider*).

un terzo, a condizione che il contratto sia a favore della persona interessata (escluso il caso delle attività svolte dalla pubblica autorità nell'esercizio dei suoi poteri); il pubblico interesse, in quanto ammesso dalla legge di uno Stato membro al quale il responsabile del trattamento è assoggettato, o dalla legislazione dell'Unione; la proposizione o l'esercizio di un'azione o di una difesa in giudizio; la necessità di salvaguardare interessi vitali della persona interessata o di un terzo, qualora la persona interessata sia fisicamente o giuridicamente incapace di prestare il consenso; la provenienza dei dati trasferiti da un registro pubblico aperto alla consultazione. Il Comitato europeo per la protezione dei dati – organismo istituito dal regolamento, composto da tutte le autorità nazionali di controllo insieme con il Garante europeo[81] – dovrà tuttavia emanare linee guida, raccomandazioni e migliori pratiche per consentire un'effettiva conformità dei trasferimenti in deroga.

Il nuovo regolamento, inoltre, rafforza considerevolmente la 'piena indipendenza' delle autorità nazionali di controllo dei dati che, come si è osservato, costituisce il perno attorno al quale ruota la motivazione della Corte di giustizia nella sentenza *Schrems*. L'art. 47, par. 1 stabilisce chiaramente che «l'autorità di controllo esercita le sue funzioni e i suoi poteri in piena indipendenza e imparzialità». Specifiche garanzie sono previste nel regolamento dal punto di vista delle prerogative che garantiscono lo *status* di indipendenza dell'*authority* rispetto allo Stato che l'ha istituita.

Resta tuttavia l'incertezza relativa alla possibile contraddittorietà delle decisioni che, nell'esercizio della loro 'piena indipendenza', le autorità nazionali di controllo possono emanare, e la questione dei termini nei quali esse devono ritenersi assoggettate alla Commissione. Basti pensare che quest'ultima, all'indomani della sentenza *Schrems*, preannunciava già l'invio di linee direttive a dette *autorithies*, per evitare applicazioni difformi in sede nazionale dei principi stabiliti dalla Corte[82].

La Corte di giustizia non sembra preoccuparsi troppo, nella sua pronuncia, della possibile contraddittorietà delle decisioni delle autorità nazionali di controllo. D'altra parte, la direttiva non si proponeva un'armonizzazione completa, ma soltanto un ravvicinamento delle legislazioni nazionali, e ammetteva quindi l'eventualità di differenze nella sua applicazione a livello nazionale. È chiaro invece che l'uniforme

[81] Cfr. artt. 64 ss. del testo provvisorio del regolamento.

[82] Cfr. il comunicato stampa della Commissione n. 15/5782 del 6 ottobre 2015: *First Vice-President Timmermans and Commissioner Jourová 's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems)*, in, in http://europa.eu/rapid/press-release_STATEMENT-15-5782_it.htm.

applicazione del regolamento non potrà essere raggiunta mantenendo l'assoluta indipendenza delle autorità di controllo. Oltre al rischio di decisioni difformi, che contrastano con la finalità stessa del regolamento, si potrebbe incentivare il «forum shopping» da parte di responsabili del trattamento non europei che, a fronte di prassi amministrative differenti a livello nazionale, potrebbero scegliere di stabilirsi in un determinato Stato membro per assoggettarsi all'autorità di controllo più compiacente o più mite. Inoltre, l'indipendenza delle autorità nazionali di controllo nell'esercizio dei loro poteri non dovrebbe impedire il loro assoggettamento all'indirizzo della Commissione. L'indipendenza delle autorità nazionali deve quindi essere necessariamente controbilanciata, in applicazione del regolamento, da una stretta cooperazione reciproca tra tutte le autorità, e tra queste e la Commissione[83].

Per quanto riguarda il coordinamento reciproco delle autorità nazionali di controllo, il nuovo regolamento stabilisce il principio definito dello «sportello unico», che prevede che, quando ad un determinato trasferimento verso Stati terzi siano applicabili le leggi di più Stati membri, o quando siano coinvolti i dati personali di interessati residenti in più Stati membri, l'autorità nazionale di controllo dello Stato nel quale si trova lo stabilimento principale del responsabile o dell'incaricato del trattamento agisca come autorità capofila per la sorveglianza delle attività di trattamento effettuate dal responsabile o dall'incaricato del trattamento *in tutti gli Stati membri*. L'autorità capofila «è l'unica autorità autorizzata a decidere in merito a misure volte a sortire effetti giuridici per quanto riguarda le attività di trattamento del responsabile del trattamento o dell'incaricato del trattamento di cui è responsabile».[84] La *leading autorithy* potrà adottare provvedimenti produttivi di effetti giuridici soltanto dopo essersi consultata con le altre autorità, sforzandosi di raggiungere un consenso comune su tali misure. A questo scopo sono previsti obblighi di assistenza reciproca tra le autorità nazionali, consistenti essenzialmente in richieste di informazioni e in misure di controllo, quali richieste di autorizzazione o di consultazione preventiva, ispezioni e indagini.

Lo specifico strumento attraverso il quale il nuovo regolamento si propone invece di coordinare le autorità nazionali di controllo con la Commissione è il cosiddetto «meccanismo di coerenza». Introdotto dall'art. 57, è un sistema che deve essere instaurato innanzitutto quando un'autorità nazionale intenda determinare *standard protection clauses*,

[83] V. Art. 46, par. 1 del testo provvisorio del regolamento.
[84] Art. 54 *bis*., par. 2 del testo provvisorio del regolamento.

autorizzare clausole contrattuali o approvare *binding corporate rules*[85]. In secondo luogo, il meccanismo di coerenza può essere attivato a richiesta della Commissione, del Comitato europeo o di un'autorità nazionale di controllo nel caso in cui l'autorità di un altro Stato membro debba affrontare 'questioni di applicazione generale', relative all'uniforme applicazione del regolamento (art. 58, par. 3). È anche prevista, in via residuale, la possibilità di instaurare un meccanismo di coerenza qualora l'autorità nazionale di controllo che assume il ruolo di capofila debba adottare misure vincolanti in casi individuali (art. 58 *bis*). Questo meccanismo prevede che, prima dell'approvazione di quasiasi misura, l'autorità nazionale di controllo ne comunichi una bozza alla Commissione, al Comitato europeo per la protezione dei dati e alle altre autorità nazionali. Il Comitato dovrà o potrà, a seconda dei casi, esprimere un parere preventivo, che verrà reso pubblico e potrà diventare vincolante sull'autorità nazionale di controllo (par. 7 dell'art. 58 *bis*). È espressamente stabilito che, qualora un'autorità nazionale di controllo violi il meccanismo di coerenza, le misure da essa adottate a seguito della violazione non saranno valide né eseguibili negli Stati membri (art. 63, par. 2).

In continuità con la direttiva, il nuovo regolamento riconferma che, in linea di principio, ciascuna autorità nazionale di controllo esercita i poteri che le sono attribuiti «sul territorio del proprio Stato membro» (art. 51, par. 1). Tuttavia, con una novità di significativo rilievo rispetto alla direttiva, come interpretata dalla Corte nel caso *Weltimmo*[86], il regolamento prevede che una misura esecutiva legittimamente adottata da un'autorità di controllo possa essere attuata in qualsiasi Stato membro, quindi anche in uno Stato diverso da quello nel quale siede l'autorità di controllo che ha preso tale decisione (art. 63, par. 1). Non è del tutto chiara, tuttavia, l'eventuale interazione di questa previsione con le condizioni per il riconoscimento e l'esecuzione delle decisioni stabilite nel regolamento «Bruxelles I *bis*».[87]

[85] V. art. 58 lett. *d, e, f* e art. 42, par. 2, lett. *c* e *d* e art. 43 del testo provvisorio del regolamento.

[86] Corte di giustizia, 1° ottobre 2015, *Weltimmo* cit., par. 60.

[87] L'art. 1, par. 1 del regolamento stabilisce che esso «si applica in materia civile e commerciale, indipendentemente dalla natura dell'autorità giurisdizionale», ma «non si estende, in particolare, alla materia […] amministrativa»: v. regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio del 12 dicembre 2012 concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (c.d. «Bruxelles I *bis*», in *G.U.U.E.* n. *L* 351 del 20 dicembre 2012, p. 1 ss.), modificato dal regolamento (UE) n. 542/2014 del Parlamento europeo e del Consiglio, del 15 maggio 2014, per quanto riguarda le norme da applicare con riferimen-

Resta ovviamente esclusa qualsiasi efficacia extraterritoriale dei poteri delle autorità nazionali di controllo rispetto a Stati terzi. In questa prospettiva, il regolamento prevede che, fatti salvi eventuali trattati internazionali di reciproca assistenza giudiziaria che vincolano l'Unione o un singolo Stato membro, non potranno essere riconosciute o dichiarate esecutive nell'Unione decisioni giurisdizionali o misure amministrative di Stati terzi, che ingiungano a un responsabile o a un incaricato del trattamento stabilito nell'Unione di divulgare il contenuto di dati personali trattati nel territorio di uno Stato membro (art. 43 *bis*) – che esigano, in definitiva, di trasferire tali dati nello Stato terzo che ha preso il provvedimento. Qualora il responsabile o l'incaricato del trattamento stabilito nell'Unione riceva un'intimazione del genere dovrà notificarla all'autorità di controllo e attendere la sua autorizzazione preventiva. Questa verrà concessa soltanto se il trasferimento può avvenire in conformità al regolamento, e se è necessario e obbligatorio per la proposizione, l'esercizio o la contestazione di azioni in giudizio (art. 44, par. 1, lett. *d* e lett. *e*) o «per importanti ragioni di interesse pubblico» , non meglio specificate. Resta fermo che l''interesse pubblico' deve essere riconosciuto dal diritto dell'Unione o dello Stato membro al quale è assoggettato il responsabile del trattamento (art. 44, par. 5).

Se sono coinvolte persone interessate che si trovano in altri Stati membri, l'autorità di controllo applicherà il meccanismo di coerenza, e in ogni caso la persona interessata dovrà essere informata dell'autorizzazione concessa dall'autorità di controllo[88]. È evidente la volontà del legislatore di evitare che i trasferimenti internazionali consentano alle autorità pubbliche di Stati terzi l'accesso ai dati senza le adeguate garanzie, esigenza ribadita dal Gruppo Art. 29, che ha già proposto un'interpretazione restrittiva di questa parte del regolamento[89].

Parallelamente, il nuovo regolamento promuove la cooperazione con Stati terzi e organizzazioni internazionali, specialmente se la Commissione

to al Tribunale unificato dei brevetti e alla Corte di giustizia del Benelux (in G.U.U.E. n. L 163 del 29 maggio 2014, p. 1 ss.).

[88] In questo senso cfr. anche la sentenza della Corte del 1° ottobre 2015, causa C 201/14, *Smaranda Bara* cit., par. 28 ss., nella quale la Corte ha stabilito che uno Stato membro non può legittimamente consentire , senza prevedere appropriate garanzie, misure che consentono a un'amministrazione pubblica di questo Stato di trasmettere dati personali a un'altra amministrazione pubblica dello stesso Stato, a fini di trattamento, senza che le persone interessate siano state informate di tale trasmissione o del successivo trattamento, in conformità ai principi stabiliti dagli artt. 10, 11 e 13 della direttiva.

[89] WP 29, *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing*, WP 232/15 del 22 settembre 2015, p. 7 s.

ritenga che essi assicurino un adeguato livello di protezione dei dati *ex* art. 41, par. 3. Tanto la Commissione, quanto le autorità di controllo dovranno sviluppare effettivi meccanismi di cooperazione internazionale per assicurare l'applicazione dei diritti e delle libertà fondamentali relativamente alla protezione dei dati personali, e offrire reciproca assistenza internazionale nell'applicazione delle relative disposizioni, comprese quelle riguardanti le notifiche, il deposito dei ricorsi, l'assistenza per l'attività istruttoria e lo scambio di informazioni (art. 45, par. 1, lett. *a* e *b*). Questo costituisce uno sviluppo innovativo, specialmente per quanto riguarda il coinvolgimento diretto nelle relazioni internazionali di organismi interni, quali sono le autorità nazionali di controllo[90].

Infine, un emendamento apposto dal Parlamento europeo al considerando 90 della proposta di regolamento vorrebbe che, qualora uno Stato terzo richieda ai responsabili del trattamento requisiti di conformità contrastanti rispetto a quelli stabiliti dal regolamento, la Commissione abbia l'obbligo di garantire che, nel conflitto di giurisdizione con lo Stato terzo interessato, il diritto dell'Unione prevalga 'in ogni circostanza'[91]. Un obbligo difficile da adempiere, tuttavia, poiché la necessaria applicazione delle norme del regolamento non può che dipendere dal tenore del diritto

[90] Inoltre, la Commissione e gli Stati membri dovranno coinvolgere le parti interessate nel dibattito e nelle attività relative alla promozione della cooperazione internazionale, promuovere lo scambio e la documentazione relativa tanto alla legislazione quanto alla prassi, fornirsi informazioni e consultarsi su conflitti di giurisdizione con Stati terzi (lett. *c, d* e *da* del par. 1 dell'art. 45 del testo provvisorio del regolamento).

[91] Cfr. risoluzione legislativa del Parlamento europeo del 12 marzo 2014 cit., emendamento n. 63 al considerando 90 del regolamento (in corsivo nel testo): «90. Alcuni paesi terzi adottano leggi, regolamenti e altri strumenti legislativi finalizzati a disciplinare direttamente le attività di trattamento dati di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. L'applicazione extraterritoriale di tali leggi, regolamenti e altri strumenti legislativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della tutela delle persone garantita nell'Unione con il presente regolamento. I trasferimenti dovrebbero quindi essere consentiti solo se ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi. Ciò vale tra l'altro quando la divulgazione è necessaria per un motivo di interesse pubblico rilevante riconosciuto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento. Occorre che la Commissione precisi le condizioni in cui sussiste un motivo di interesse pubblico rilevante con un atto delegato. *Laddove i responsabili del trattamento o gli incaricati del trattamento si trovino di fronte a requisiti di conformità contrastanti tra la giurisdizione dell'Unione, da una parte, e quella di un paese terzo, dall'altra, la Commissione deve garantire che il diritto dell'Unione prevalga in ogni circostanza. La Commissione ha il compito di fornire consulenza e assistenza al responsabile del trattamento e all'incaricato del trattamento nonché di cercare di risolvere il conflitto di giurisdizione con il paese terzo interessato*.»

internazionale privato dello Stato che esercita la giurisdizione nella relativa controversia. Se, nella fattispecie, fosse giurisdizionalmente competente lo Stato terzo, è evidente che difficilmente la Commissione potrebbe influire sull'obbligo dell'autorità amministrativa o dell'organo giudicante dello Stato terzo di determinare la legge applicabile al trattamento sulla base delle regole di applicabilità, o del diritto internazionale privato, in forza nello Stato terzo nel quale tale autorità o tale giudice siede.

Conclusioni

La sentenza *Schrems* riflette con chiarezza le preoccupazioni della Corte di giustizia a causa dell'inefficacia di fatto del sistema predisposto dall'Unione per la protezione dei dati personali trasferiti verso Stati terzi.

L'aspetto sconcertante di questa vicenda è che non vi sono stati inadempimenti formali rispetto agli obblighi di legge incombenti sul *service provider,* eppure gravissime violazioni del diritto fondamentale alla protezione dei dati personali hanno potuto verificarsi, senza che questo incidesse sulla continuità del flusso dei dati verso gli Stati Uniti. L'inefficacia del sistema di tutela è tanto più grave, in quanto non riguarda soltanto la decisione relativa al «Safe Harbor» o la direttiva 95/46/CE, ma lo stesso diritto primario relativo alla protezione dei dati personali, cioè il Trattato sul funzionamento dell'Unione europea e la Carta dei diritti fondamentali dell'Unione europea.

E se la principale responsabilità per tale situazione dev'essere addebitata alla decisione relativa al «Safe Harbor», che ha meritato di essere dichiarata invalida, tuttavia anche le altre decisioni di adeguatezza emanate dalla Commissione risultano discutibili, per motivi diversi. Infatti, anche a voler prescindere dal merito della valutazione relativa all'adeguatezza sostanziale della protezione garantita dai vari Stati, queste decisioni si sono rivelate di scarsissimo rilievo pratico, ai fini della promozione della libertà di circolazione internazionale dei dati, che pure dovrebbe rappresentare un obiettivo prioritario per la Commissione, come evidenziano tanto il piano d'azione per l'attuazione dell'«Agenda digitale europea», quanto la strategia «Europa 2020»[92]. Pertanto, tutto il sistema relativo

[92] Cfr. Commissione, doc. COM(2012)11 def. - 2012/0011(COD) cit., p. 2, par. 1, in riferimento alla Comunicazione della Commissione *Un'agenda digitale europea*, COM(2010) 245 def. del 19 maggio 2010; Comunicazione della Commissione *EUROPA 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva*, COM(2010)2020 def. del 3 marzo 2010.

al trasferimento dei dati personali dall'Unione europea verso Stati terzi sembra aver fallito l'una o l'altra delle proprie finalità, e cioè la tutela delle persone quanto al trattamento dei dati personali e il rafforzamento della libertà di circolazione dei dati come strumento per la promozione della competitività delle imprese europee nel mercato interno e nel commercio internazionale.

A fronte delle falle del sistema, tuttavia, il nuovo regolamento non introduce apparentemente modifiche sostanziali alla disciplina del trasferimento dei dati verso Stati terzi. Il principio generale resta sempre quello dell'autorizzazione condizionata, con la dichiarazione di adeguatezza della Commissione relativa al livello di protezione garantito dallo Stato terzo, oppure con la decisione di non adeguatezza; sono ancora consentiti gli strumenti giuridici vincolanti per trasferire i dati verso Stati terzi che non assicurino un adeguato livello di protezione; ed è ancora prevista la possibilità di trasferimenti in deroga.

Andando oltre le apparenze, tuttavia, la prospettiva è rovesciata: se la direttiva istituiva un rapporto da regola a eccezione tra i trasferimenti effettuati sulla base della decisione di adeguatezza della Commissione, e quelli effettuati sulla base di strumenti giuridici vincolanti, il nuovo regolamento stabilisce, tra questi e i trasferimenti basati sulle decisioni di adeguatezza, una relazione che si avvia a diventare paritaria. Il punto di vista del legislatore è chiaro: la garanzia della protezione dei dati nei trasferimenti internazionali non può più essere assicurata esclusivamente da un processo di conformità con il sistema normativo, isolatamente considerato, come ha evidenziato peraltro anche il caso *Schrems*. Gli obblighi legislativi devono trovare necessariamente corrispondenza negli obblighi vincolanti di autoregolamentazione imposti al responsabile del trattamento: in altri termini, la protezione dei dati personali nei trasferimenti internazionali deve essere il risultato di una cooperazione tra l'azione del legislatore, che resta ancora il principale soggetto sul quale grava la responsabilità di garantire la legittimità del trasferimento, e l'azione del responsabile del trattamento, in assolvimento di obblighi di *self-regulation* posti direttamente in capo ad esso, sotto la vigilanza delle autorità di controllo.

In questa prospettiva, quasi in risposta alle richieste della Corte di giustizia, il regolamento rafforza considerevolmente l'indipendenza delle autorità nazionali di controllo. Tuttavia, per quanto piena e completa possa essere l'indipendenza delle *authorities*, questa non le esime dalla necessità di coordinarsi reciprocamente, né dall'obbligo di assoggettarsi all'autorità della Commissione, al fine di non vanificare l'applicazione uniforme del

regolamento a livello nazionale. L'esigenza di conciliare questi aspetti potenzialmente conflittuali è ben conosciuta dal legislatore dell'Unione che, in altri casi – ad esempio, nell'applicazione del diritto della concorrenza[93] – ha risolto il problema attraverso la creazione di una rete europea di cooperazione tra la Commissione e le autorità garanti degli Stati membri. Il regolamento, pur senza istituire una formale rete di cooperazione, interviene con modalità analoghe a quelle previste per l'*enforcement* della concorrenza: da un lato estende anche alla materia del trasferimento dei dati il principio del cosiddetto 'sportello unico', con un'autorità capofila, qualora più autorità nazionali di controllo rivendichino una competenza nello stesso caso; dall'altro, istituisce un 'meccanismo di coerenza', nel quale sono coinvolte tanto le autorità nazionali e il Comitato europeo per la protezione dei dati, quanto la Commissione – la cui funzione di guida peraltro non appare ancora del tutto chiara[94].

Ma la questione forse più critica riguarda l'eventuale esecutività dei provvedimenti delle autorità nazionali di controllo nel territorio di Stati diversi da quello nel quale siedono le autorità che li hanno emanati. In applicazione della direttiva, questo effetto è stato esplicitamente respinto dalla Corte di giustizia nella sentenza *Weltimmo*, che ha preceduto di pochi giorni la sentenza *Schrems*. Il testo provvisorio del regolamento, invece, stabilisce espressamente che le decisioni esecutive delle autorità nazionali di controllo possano avere efficacia in tutti gli Stati membri dell'Unione europea. Resta esclusa, ovviamente, la portata extraterritoriale di tali provvedimenti al di fuori dell'Unione. Allo stato attuale del diritto internazionale[95], non sembra possibile ottenere questo risultato se non attraverso la conclusione di specifici accordi con gli Stati interessati. Tuttavia, con un'omissione che è stata già evidenziata dal Garante europeo per la protezione dei dati, il regolamento non impone la revisione degli accordi internazionali conclusi dall'Unione nella materia del trasferimento dei dati, allo scopo di allinearli al regolamento[96].

[93] Cfr. la Comunicazione della Commissione sulla cooperazione nell'ambito della rete delle autorità garanti della concorrenza, in *G.U.U.E.*, C 101 del 27 aprile 2004, p. 43 ss.

[94] Peraltro, il ruolo di guida attribuito alla Commissione non è del tutto chiaro, poiché sembra che la Commissione si limiti, nella fase iniziale, ad attivare il ricorso al Comitato (art. 58, par. 4) e, in una fase successiva, abbia soltanto il potere di adottare pareri.

[95] Anche l'Assemblea delle Nazioni Unite ha recentemente sottolineato che il diritto umano alla privacy deve godere anche nello spazio digitale dell'identica tutela che gli è offerta nel mondo reale: cfr. risoluzione dell'Assemblea ONU 68/17 del 18 dicembre 2013, intitolata «*The Right to Privacy in the Digital Age*» (A/RES/68/167 -A/68/456/Add.2), in http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167).

[96] Cfr. Garante europeo della protezione dei dati, Parere del 7 marzo 2012 sul

Tra gli accordi conclusi dall'Unione, vi è, in particolare, quello firmato con gli Stati Uniti nel 2012, recante *Trade Principles for Information and Communication Technology Service*[97]. Questo accordo, avente valore dichiarativo e non vincolante, trova applicazione nel settore delle reti e dei servizi per le tecnologie dell'informazione e della comunicazione, sia nell'ambito delle relazioni commerciali bilaterali tra Unione europea e Stati Uniti, sia nel quadro dei negoziati internazionali eventualmente aperti da questi con Stati terzi, senza pregiudizio degli obblighi internazionali sanciti dal WTO e dal GATS. Ispirati ai *Principles on Internet Policymaking* dell'OCSE[98], gli orientamenti stabiliti da questo accordo impegnano gli Stati contraenti, in particolare, a non ostacolare i trasferimenti internazionali di dati effettuati da *service providers* stabiliti in altri Paesi o dai loro clienti, e a non bloccare l'accesso, da parte degli stessi *service providers* o dei loro clienti, alle informazioni pubblicamente disponibili, o alle informazioni di loro proprietà conservate in altri Paesi.

Questo accordo è tuttavia destinato ad essere superato dal discusso accordo di libero scambio tra Unione europea e Stati Uniti, attualmente è in corso di negoziazione («Transatlantic Trade and Investment Partnership» o «TTIP»)[99]. Le perplessità suscitate presso una larga parte dell'opinione pubblica dalle trattative relative a questo accordo dipendono dal fatto che il testo sembra consentire, nelle materie che ne sono oggetto, un'applicazione significativamente attenuata delle disposizioni dell'Unione relative alla protezione dei dati personali.

Si noti, in proposito, che il GATS non vieta, in linea di principio, di apporre barriere allo scambio internazionale di servizi giustificate dalla

pacchetto di riforma della protezione dei dati (2012/C 192/05), in G.U.U.E., C 192 del 30 giugno 2012, p. 7 ss., a proposito del considerando 79 del regolamento.

[97] *European Union-United States Trade Principles for Information and Communication Technology Service*, accordo concluso in data 4 aprile 2012, in http://trade.ec.europa.eu/doclib/docs/2011/april/tradoc_147780.pdf : «*3. Cross-Border Information Flows: Governments should not prevent service suppliers of other countries, or customers of those suppliers, from electronically transferring information internally or across borders, accessing publicly available information, or accessing their own information stored in other countries.*»

[98] OECD (*Organization for Economic Cooperation and Development* – Organizzazione per la Cooperazione e lo sviluppo economico), *Recommendation of the OECD Council on Principles for Internet Policy Making*, C(2011)154 del 13 dicembre 2011, in http://www.oecd.org/internet/ieconomy/49258588.pdf (pubblicati nel 2014 in versione finale: OECD *Principles on Internet Policy Making*, in http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf). In dottrina, cfr. R.H. Weber, *Principles for Governing the Internet: A Comparative Analysis*, 6th ed., Paris, 2015.

[99] V. la pagina dedicata alle trattative in corso sul sito della Commissione: http://ec.europa.eu/trade/policy/in-focus/ttip/.

protezione dei dati personali[100]. Da questo punto di vista, l'Unione europea non infrangerebbe quindi alcun obbligo internazionale, se assicurasse, anche nei rapporti commerciali con Stati terzi, il diritto fondamentale delle persone alla protezione dei propri dati.

Tuttavia, al di là dell'aspetto formale, è evidente che un livello di tutela così elevato come quello richiesto dalla Corte di giustizia nella sentenza *Schrems* comporta un rischio di frammentazione del mercato globale dell'informazione, che può effettivamente tradursi in un concreto ostacolo alla competitività internazionale delle imprese stabilite nell'Unione europea.

Il punto di equilibrio tra queste opposte esigenze non dovrebbe tuttavia essere ricercato abbassando il livello di protezione dei dati personali negli scambi commerciali con Stati terzi. Al contrario, come indicato anche dal nuovo regolamento, la strada da seguire non può che essere quella di instaurare iniziative a livello internazionale per estendere il diritto alla protezione nel trattamento dei dati personali, come *standard* non più rinunciabile da parte del legislatore[101].

[100] Il General Agreement on Trade in Services («GATS») ammette, tra le eccezioni generali all'applicazione delle sue disposizioni, «the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts»: v. l'Art. XIV(*c*)(*ii*), entrato in vigore il 1° gennaio 1995 (in https://www.wto.org/english/docs_e/legal_e/26-gats.pdf): «Subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: […]; c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: […]; (*ii*) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts; […]». Nessuna decisione del Panel ha finora interpretato l'Art. XIV(c)(ii). Invece, nel quadro del WTO (*World Trade Organization*), esiste un *Work Programme on Electronic Commerce*, adottato dal General Council il 25 settembre 1998, (doc. WT/L/274, 30 September 1998, 98-3738 in https://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm, adottato a seguito della *Geneva Ministerial Declaration on Global Electronic Commerce* del 20 maggio 1998 (WT/MIN (98)/DEC/2, 92-2148, 25 May 1998, in https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm), che elenca, tra le questioni che il *Council for Trade in Services* dovrà esaminare, *«protection of privacy and public morals and the prevention of fraud (Article XIV)»* (par. 2.1). In dottrina, cfr., per tutti, M.V. Pérez Asinari, *Is There Any Room for Privacy and Data Protection Within the WTO Rules?, in The Electr. Commun.* Law Rev., 2002, p. 249 ss.

[101] Sull'influenza della disciplina europea sulle iniziative promosse a livello internazionale in relazione alla protezione dei dati personali, cfr. G. Greenleaf, *The Influence*

Abstract

This paper examines the EU Court of justice's judgment in the case Maximillian Schrems v. Data Protection Commissioner. In this landmark ruling, the Court declares that the European Commission's decision enforcing the «Safe Harbor» agreement between the US Department of Commerce and the European Union, read in the light of Articles 7, 8 and 47 of the EU Charter of Fundamental Rights, is invalid. Although the Commission found that the American legal system affords an adequate level of protection of personal data, the Court holds that the law and practices in force in the USA at the time of the facts of the case did not ensure a protection sufficient to comply with the requirements of the EU legislation on the protection of such data. The Court further determines that national supervisory authorities of Member States may examine claims concerning violation of an individual's rights in regard to the processing of his personal data which has been transferred to a third country.

The analysis of the judgement is conducted in two parts. The first briefly presents the basic elements of the case and outlines the fundamental requirements of directive 95/46/CE (the «General Data Protection Directive») and its mechanism of transfers of personal data to third countries. The second part identifies the reasons of the Court's decision and discusses some of the problematic consequences raised by the case. These include the effective functioning of the EU data protection law and the Charter of Fundamental Rights; the «complete independence» of functions of Member States' national supervisory authority; the Commission's power to adopt adequacy decisions regarding third States; the legal effects of the declaration of invalidity of the «Safe Harbor» decision and its disruptive practical consequences on transatlantic data transfers.

The issues raised by the Court's ruling are also examined under the new General Data Protection Regulation's draft text, since the European institutions have reached agreement on this important measure, which is due to abrogate and substitute the directive.

A further scrutiny is devoted to the new Commission's proposal for a «EU-US Privacy Shield», which is intended to substitute the «Safe Harbor» decision.

The comment concludes with a brief general assessment of the questions that the judgment of the Court leaves open, and some observations regarding the tense relationships with the USA because of the tentative assertion by the EU legislator of its data protection legal framework as a model legislation at a global level.

of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, in *Intern. Data Privacy Law*, 2012, p. 68 ss.

Giovanni Maria Riccio

Model Contract Clauses *e* Corporate Binding Rules*: valide alternative al* Safe Harbor Agreement*?*

Sommario: Introduzione. – 1. Scambi di dati tra Europa e Stati Uniti e impatto economico della decisione. – 2. Il complesso rapporto tra Europa e Stati Uniti su tutela dei dati personali ed esigenze di sicurezza. – 3. *Corporate Binding Rules*. – 4. *Model Contract Clauses*. – 5. L'immodificabilità delle clausole e la soluzione inglese. – 6. Rapporti tra importatore ed esportatore. – Conclusioni.

Introduzione

La decisione della Corte di Giustizia del 6 ottobre 2015, che ha invalidato gli accordi cc.dd. *safe harbor* (2000/520/EC), si presta a molteplici letture. È indiscutibile, però, che rapportarsi a tale pronuncia sulla scorta della mera analisi giuridica rischia di offrire uno scenario parziale, senza dare compiutamente atto delle complesse e intricate vicende che hanno accompagnato prima l'emanazione e poi l'invalidazione di tali accordi. Accordi, pare opportuno ricordarlo, che erano in corso di revisione e che, al momento della decisione dei giudici comunitari, stavano evidenziando una lettura della tematica differente tra le istituzioni europee e quelle statunitensi.

Prima di addentrarci nell'analisi di tali aspetti, alcuni dei quali saranno solo abbozzati in tale sede, considerando che verranno affrontati da altri saggi pubblicati nel presente numero monografico, giova ripercorrere brevemente la funzione di tali accordi nel contesto normativo del trasferimento dei dati personali al di fuori dello spazio europeo.

È noto che l'art. 25 della direttiva n. 46/95/CE prevede un generale divieto di trasferire dati personali al di fuori dell'Unione europea.

Questa regola ammette, però, una serie di eccezioni: il trasferimento è consentito nel caso in cui vi sia il consenso della persona cui i dati personali si riferiscono oppure avvenga in esecuzione di misure contrattuali o precontrattuali o, ancora, per rispondere ad un interesse pubblico; in

presenza di strumenti negoziali, validati dalla Commissione europea, che offrano garanzie di sicurezza; infine, in caso di decisioni di adeguatezza, oppure decisioni della Commissione europea che attestino che un determinato Paese, non appartenente all'Unione europea o allo Spazio economico europeo, assicuri un livello di protezione 'adeguato' ossia sia dotato di misure legislative, nonché tecniche e di sicurezza, che offrano un grado di tutela dei dati personali conforme agli standard comunitari[1].

Tra le decisioni di adeguatezza – che hanno interessato, tra gli altri, Israele, Svizzera, Australia e Canada – la più nota è quella del 26 luglio 2000 tra Unione europea e Stati Uniti, annullata dalla sentenza oggetto del presente scritto e sostituita, nel febbraio del 2016, dai nuovi accordi, denominati *EU-US Privacy Shield*.

Le ipotesi, pertanto, in cui sussiste la legittimazione al trasferimento dei dati personali all'estero possono essere riassunte in due macroaree: una prima ipotesi in cui la legittimazione discende da un'intesa tra istituzioni pubbliche (la Commissione europea e singoli Stati terzi, non appartenenti all'Unione europea); l'altra ipotesi che trova fonte, invece, nell'autonomia privata, seppur integrata dalle prescrizioni legislative.

All'interno di questa seconda macroarea occorre poi distinguere l'ipotesi in cui sia lo stesso soggetto interessato a prestare il proprio consenso, *in maniera inequivocabile* al trasferimento del dato (art. 26, par. 1, lett. *a)* della direttiva), da quella in cui sia stata la Commissione europea ad approvare gli accordi interni alle imprese (nel caso delle *corporate binding rules*) o, in alternativa, a dettare le clausole da recepire nei contratti di esportazione dei dati personali (nel caso delle *model contract clauses*).

1. Scambi di dati tra Europa e Stati Uniti e impatto economico della decisione

In via preliminare, ancor prima di occuparci di tali strumenti alternativi agli accordi di adeguatezza, occorre però esaminare alcuni profili che,

[1] G. Finocchiaro, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna-Roma, 2012, p. 283, sottolinea correttamente che la legge italiana ha invertito l'approccio della direttiva comunitaria. Difatti, «*la legge italiana vieta all'art. 45 il trasferimento all'estero se l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato e lo consente se ricorrono alcune specifiche circostanze individuate negli artt. 43 e 44 del Codice*», *la direttiva, invece,* «*dispone che i dati personali possono essere trasferiti dall'Europa verso Paesi extraeuropei, se i Paesi di destinazione garantiscono un adeguato livello di sicurezza*».

sebbene alieni dalla stretta analisi giuridica, consentono di comprendere appieno le sfaccettature intricate della fattispecie in esame.

Difatti, sebbene la sentenza della Corte di Giustizia abbia ricevuto apprezzamenti da più parti, non da ultimo dal nostro Garante per la protezione dei dati personali[2], che ha sottolineato l'importanza del rispetto dei diritti dei cittadini anche al di fuori dei confini comunitari, si è al cospetto di opinioni che, seppur astrattamente condivisibili, fotografano solo una faccia di un prisma molto più complesso.

Non può essere sottaciuto, infatti, l'impatto economico e politico della sentenza Schrems.

Non si tratta di una sentenza che colpisce Facebook, Google o altri 'colossi' della *new economy*, come semplicisticamente si è detto: sono oltre quattromila le imprese europee e statunitensi che hanno beneficiato dei principi di *Safe Harbor* e, di queste, circa il 60% sono piccole e medie imprese, incluse numerose start-up. Allo stesso modo, non deve dimenticarsi come l'utilizzo della rete internet – che ha catalizzato l'allarme associato al trasferimento dei dati – abbia incrementato fortemente le esportazioni da parte delle imprese medie e piccole, che hanno sfruttato le opportunità date dalla possibilità di offrire a costi contenuti i propri prodotti al di fuori dei confini nazionali[3].

Le relazioni commerciali tra imprese statunitensi ed europee sono le più importanti del mondo, in termini numerici e di fatturato: basti pensare che 61% delle importazioni statunitensi proviene da scambi commerciali con imprese europee e il 33% delle importazioni comunitarie proviene dagli Stati Uniti[4]. Sono dati destinati a crescere e che dipendono anche dall'accresciuta fiducia e dimestichezza degli utenti con gli acquisti on-line[5] e dalla penetrazione di internet nella popolazione, che negli Stati

[2] Garante per la protezione dei dati personali, *Facebook: dichiarazione di Antonello Soro sulla sentenza della Corte di Giustizia Europea*, 6 ottobre 2015, Doc. web 4308245.

[3] Al riguardo, è interessante la lettura del report pubblicato da eBay, la più grande piattaforma di aste on-line e uno dei maggiori operatori di e-commerce, secondo cui il 95% delle PMI statunitensi che utilizzano i propri servizi ha esportato i prodotti commercializzati, a fronte di una percentuale pari al 5% delle imprese che non operano *on-line*. Allo stesso modo, se si comparano le imprese che continuano ad esportare a tre anni dalla prima transazione, si registra che il 75% di queste operano *on-line*, mentre solo 15% delle PMI che non utilizzano internet riesce a mantenere le esportazioni nel medesimo arco temporale, cfr. eBay, 2015 *US Small Business Global Growth Report*, 2015.

[4] Cfr. D.S. Hamilton – J.P. Quinlan, *The Transatlantic Economy 2014*, Vol. 1, 2014. Nel 2014, il valore delle esportazioni statunitensi verso l'Unione Europea è stato di oltre 219 miliardi di dollari; le importazioni dall'Europa pari a 169 miliardi di dollari.

[5] Dal 2011 al 2013, l'e-commerce negli Stati Uniti è cresciuto da $ 13.630.000.000

Uniti ha raggiunto l'83% e in Europa oscilla dal 90% del Regno Unito al 60% dell'Italia, a fronte di una media mondiale pari ad appena il 32%[6].

Come è facile immaginare, la maggiore diffusione di internet si traduce anche in un aumento dei dati[7], non necessariamente di natura personale, scambiati per mezzo delle infrastrutture (reti terresti o cavi sottomarini): anche in questo caso, l'esame del flusso dei dati evidenzia che la maggiore mole di trasferimenti avviene tra Europa e Stati Uniti[8].

Peraltro, in molti casi, il transito dei dati è solo temporaneo e dipende dalla localizzazione dei sistemi informatici adoperati; in altri casi, invece,

a $ 42.130.000.000 e dovrebbe raggiungere $ 133.000.000.000 di fatturato entro il 2018, cfr. Statista Dossier, *Global Internet Usage* 2014, 47. Cfr. anche J.F. Gonzales – J. Bradford – K. Yunhee – K.N. Hildegunn, *«Globalisation of Services and Jobs»*, in *Policy Priorities for International Trade and Jobs* (OECD 2012), 186.

[6] Sul punto si rinvia a J.P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment, Brookings Working Paper* 79, October 2014, 5.

[7] Cfr., al riguardo, il *Considerando 4* della Proposta di Regolamento Generale sulla tutela dei dati personali: «The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows. The exchange of data between public and private actors, including individuals, associations and undertakings across the Union has increased», nonché il *Considerando 5*: «Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased spectacularly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data» e il *Considerando 78*: «Cross-border flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international co- operation. The increase in these flows has raised new challenges and concerns with respect to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of individuals guaranteed in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer may only take place if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V are complied with by the controller or processor».

[8] cfr. J.P. Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment*, cit., cfr. in particolare la mappa pubblicata a pag. 6, dove si rappresenta che lo scambio dei dati tra Europa e Stati Uniti è pari al doppio di quelli che avvengono tra Stati Uniti e Cina.

il trasferimento dei dati è funzionale solo a ragioni di sicurezza (si pensi, ad esempio, alla duplicazione dei dati e all'utilizzo di server in diversi continenti, al fine di prevenire i rischi connessi alla perdita o alla distruzione dei dati personali). A riprova di quanto si sostiene, basti riflettere sui servizi di *cloud*, nei quali il trasferimento dei dati, caricati dagli utenti sulla piattaforma ai fini della conservazione o della condivisione degli stessi, rappresenta il corollario del servizio principale offerto dalle imprese del settore. Servizi che, è opportuno rimarcarlo, si riverberano anche sulla produttività dei lavoratori e sull'efficienza dei servizi forniti dalle imprese[9].

Alla luce di tali dati, pare possibile concludere (ma trattasi di conclusione ovvia) che il flusso transfrontaliero dei dati non può essere impedito. Ciò determinerebbe la paralisi per molte imprese, tacendo il potenziale isolamento commerciale per l'Europa: una ricerca del 2013 di *Syntech Numérique* dimostra, con chiarezza, che l'interruzione del flusso dei dati transfrontalieri porterebbe alla riduzione del PIL dell'Unione europea del 1,3% e un'emorragia nelle esportazioni dei servizi forniti dall'Europa verso gli Stati Uniti, che diminuirebbero del 6,7%. Il punto, quindi, è che le imprese che intendono (o che sono costrette) ad esportare dati personali sono indotte a ripiegare, sino alla nuova decisione di adeguatezza, sulle clausole contrattuali standard – unico strumento 'sopravvissuto' al crollo del *safe harbor* –, il cui costo verrà sopportato da tutti i soggetti interessati, con un impatto differente su piccole e grandi imprese.

In tale ottica, del resto, pare possa essere spiegato anche il motivo che ha indotto le autorità comunitarie e statunitensi ad accelerare il processo di revisione – seppur per *key-point* – degli accordi e, quindi, giustificata la fretta che ha guidato alla prima bozza del *Privacy Shield* e all'adesione, probabilmente non del tutto convinta, che gli Stati Uniti hanno prestato a questo 'scudo' normativo.

[9] M. Falk – E. Hagsten, *E-Commerce Trends and Impacts Across Europe*, UNCTAD Discussion Paper No. 220, March 2015, UNCTAD/OSG/DP/2015/2, 2015; United States International Trade Commission, *Digital Trade in the U.S. and Global Economies*, Part 2 Pub. 4485 Investigation No. 332-540, 2014, 71.

2. Il complesso rapporto tra Europa e Stati Uniti su tutela dei dati personali ed esigenze di sicurezza

Si è detto in apertura che la sentenza Schrems non può essere incasellata in un'unica lettura. Sarebbe, quindi, un errore (metodologico ed ermeneutico) valutare la fondatezza della sentenza stessa alla luce della mera ripercussione negativa che essa produce sul piano economico.

Il tema, difatti, è complesso e non può essere circoscritto a una visione semplicistica, che tenderebbe a legittimare soluzioni che siano pensate nell'interesse esclusivo degli operatori economici. Il conflitto tra diritti fondamentali – quello delle imprese, da un lato, e quello dei cittadini, dall'altro – allo stesso modo, non può essere ingabbiato in una prospettiva statica, finalizzata ad evidenziare la supremazia di un diritto su di un altro: è evidente che quelli connessi alla tutela dei dati personali dei singoli sono costi sociali che le imprese devono prevedere, così come, in passato, hanno considerato, ad esempio, i costi per la sicurezza sociale dei lavoratori[10]. Sarebbe banalizzante, quindi, demarcare i confini della discussione nel rapporto tra costo di impresa e sicurezza dei dati dei cittadini.

Analogamente, la natura *lato sensu* politica della decisione della Corte di Giustizia non è sfuggita ai primi commentatori[11].

Innanzi tutto, come si accennava, la protezione dei dati personali – dopo l'approvazione Carta di Nizza – ha assunto un valore di rango costituzionale e, in tale processo di 'costituzionalizzazione', la Corte di Giustizia, nei casi *Digital Ireland*[12], *Google Spain*[13] o ora in *Schrems*, sta

[10] K. Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, *Stan. Tech. L. Rev.* 1 (2000); J.E. Cohen, *What Privacy is For?*, 126 *Harv. L. Rev.* 1904 (2003). Un recente studio ha analizzato (criticamente) l'aumento dei costi per le imprese che potrebbero scaturire a seguito dell'approvazione del Regolamento generale in materia di dati personali: L. Christensen – A. Colciago – F. Etro – G. Rafert, *The Impact of the Data Protection Legislative Framework in the E.U.*, Intertic Policy Paper, 2013.

[11] Cfr. L. Bolognini, *Una sentenza politica che non stupisce*, in *Formiche*, novembre 2015, 50; M. Mensi, *Il vero sconfitto è la Commissione europea*, *ivi*, 52; V. Zeno-Zencovich, *Serve un approccio meno ideologico*, *ivi*, 56.

[12] Corte di giustizia, 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications,* cause riunite C-293/12 e C-594/12, in *Nuova giur. civ. comm.,* 2014, I, 1044, con nota di C.M. Cascione, *I diritti fondamentali prevalgono sull'interesse alla sicurezza: la decisione* data retention *della Corte di giustizia e gli echi del datagate*, ma sul tema, in generale, v., tra gli altri, T. Konstadinides, *Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem*, in *Eur. L. Rev.*, 2011, 722.

[13] Corte di giustizia, 13 maggio 2014, *Google Spain SL e Google Inc. c. Agencia Española*

giocando un ruolo fondamentale nel progressivo ampliamento dei margini di tutela riconosciuti ai cittadini comunitari e sulla reinterpretazione della normativa comunitaria in materia di privacy (a partire dalla direttiva 96/47/CE) alla luce dei principi fissati dagli artt. 7 e 8 della Carta[14].

L'interventismo della Corte di Giustizia solleva, peraltro, l'intricato tema dei rapporti e delle competenze degli organi comunitari. Le pronunce giudiziarie in materia di *data retention* e diritto all'oblio, seppur in larga parte condivisibili, hanno aperto 'voragini' interpretative, costringendo gli operatori commerciali e le autorità garanti nazionali ad un adeguamento che, però, a ben vedere, si è tradotto in un, sia consentito il termine, 'rattoppo' della disciplina vigente più che ad un suo radicale ripensamento. Le decisioni della Corte, inevitabilmente, hanno evidenziato i punti critici dell'assetto normativo, ma non hanno offerto soluzioni applicative: soluzioni che coinvolgono, in primo luogo, le competenze della Commissione, impegnata nel difficile iter di approvazione del Regolamento in materia di dati personali, spesso pregiudicato, come per il diritto all'oblio, dalle censure della Corte di Giustizia[15].

Similmente, la sentenza *Schrems* apre delle falle cui si sta tentando di rimediare in tempi ristretti, al fine di scongiurare i danni economici di cui si diceva dinanzi, ripensando *ex novo* e con mutati rapporti di forza, i negoziati che hanno coindotto al *Privacy Shield*.

Il conflitto che si è inasprito, ma che è aperto da tempo, sta evidenziando una visione sostanzialmente antitetica tra Stati Uniti ed Europa in materia di protezione dei dati personali, da un lato, e di sorveglianza e sicurezza nazionale, dall'altro. Il caso Microsoft, deciso dalla *Second Circuit Court of Appeals* di New York e criticato apertamente dalla Commissione europea, sulla richiesta, ai sensi dello *Stored Communications Act* del

de Protección de Datos (AEPD) e Mario Costeja González, causa C-131/12, su cui si rinvia ai numerosi commenti pubblicati in *Dir. Inf.* n. 4-5, 2014, ora raccolti in G. Resta - V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su internet dopo la sentenza Google Spain*, Roma, 2015.

[14] Su tale profilo, che in questa sede può essere solo accennato, si rinvia ai contributi di O. Pollicino e M. Bassini e di G. Resta in questo Volume, con i riferimenti *ivi* menzionati.

[15] La tematica dei rapporti tra Corte di Giustizia e Commissione europea è stata ampiamente indagata dalla dottrina: cfr., tra gli altri, G. de Burca – J.H.H. Weiler, *The Worlds of European Constitutionalism*, Cambridge Univ. Press, 2011 (in particolare G. de Burca, *The ECJ and the international legal order: a re-evaluation*); M. Dawson – B. De Witte – E. Muir, *Judicial Activism At The European Court Of Justice*, Elgar Publ., London, 2013.

1986[16], di produzione di e-mail archiviate su server localizzati in Irlanda[17], è solo la punta dell'iceberg di un rapporto privacy/sicurezza che, anche a livello costituzionale, sta segnando una cesura netta tra le due sponde dell'Atlantico[18].

Una punta dell'iceberg che, tuttavia, dimostra che la raccolta indiscriminata di dati personali (c.d. *bulk metadata collection*), agevolata dal contesto normativo statunitense (specialmente con l'emanazione del *Patriot Act*[19], ma già con il *Foreign Intelligence Surveillance Act - FISA*[20]), non è arginata neanche dal potere giudiziario[21], spesso invocato come ultimo baluardo per le libertà dei cittadini[22].

[16] 18 U.S.C. §§ 2701–2712.

[17] *In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), 15 F. Supp. 3d 466 (No. 13-MJ-2814). Sul caso in questione, si rinvia a T.J. McIntyre, *Implementing Information Privacy Rights in Ireland*, in S. Egan (ed.), *International Human Rights: Perspectives from Ireland,* Dublin, Bloomsbury, 2015, 272 (articolo interessante, anche perché indaga il rapporto tra il diritto irlandese, i recenti casi decisi dalla Corte di Giustizia e l'importanza assunta dall'Irlanda nel settore che ci interessa, poiché Stato in cui molte delle società della *new economy* hanno scelto di stabilire le proprie sedi europee. Un'importanza che, come l'A. osserva, potrebbe essere accresciuta dal meccanismo *one stop shop* contenuto nel Regolamento comunitario.

[18] S.J. Shackelford, *Fragile Merchandise: A Comparative Analysis of the Privacy Rights for Public Figures*, 49 *Am. Business L. J.* 125, 132 (2012); J.Q. Whitman, *The Neo-Romantic Turn*, in P. Legrand – R. Munday (eds.), *Comparative Legal Studies: Traditions and Transitions*, Cambridge Univ. Press, 2003, 330.

[19] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Public Law Pub.L. 107–56.

[20] Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C. Ch. 36.

[21] Si pensi, ancor prima, al caso *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143 (2013), in cui la Corte Suprema ha rigettato le richieste degli attori perché «they were likely to be targets of surveillance were based too much on speculation and on a predicted chain of events that might never occur, so they could not satisfy the constitutional requirement for being allowed to sue». Il caso riguardava la possibilità riconosciuta, in base al *FISA Amendments Act of 2008*, alla *Foreign Intelligence Surveillance Court* di sorvegliare cittadini stranieri senza dover dimostrare che gli stessi rappresentassero un'effettiva minaccia, con margini operativi ritenuti dai ricorrenti eccessivamente ampi e incostituzionali. I commenti della dottrina alla decisione sono stati tendenzialmente negativi: A. Butler, *Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance*, 48 *New England L. Rev.* 56 (2013); N.M. Richards, *The Dangers of Surveillance*, 126 *Harv. L. Rev.* 1934, 1944 (2013); *contra* però A. Rubow, *Standing in the Way of Privacy Protections: The Argument for a Relaxed Article III Standing Requirement for Constitutional and Statutory Causes of Action*, 29 *Berkeley Tech. Law J.* (2014).

[22] Sulla questione, per ulteriori approfondimenti, si rinvia al saggio di G. Resta in questo Volume, ma v. già F. Bignami – G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 *Law & Cont. Probl.* 101, 108. Un'opinione diametralmente opposta è

Né può ritenersi che l'emanando *Judicial Redress Act*[23], attualmente in fase di discussione e approvazione al Senato, possa essere una risposta appagante alla decisione della Corte di Giustizia. Il JRA, infatti, si limiterebbe ad estendere ai cittadini europei i medesimi diritti riconosciuti dal *Privacy Act* ai cittadini americani in caso di violazioni dei dati personali: una soluzione comunque non idonea a frenare le preoccupazioni che hanno condotto alle censure della Corte di Giustizia, atteso che il *Privacy Act* offre garanzie insufficienti in caso di sorveglianza di massa[24].

Ma, soprattutto, una soluzione che dimostra un approccio contrapposto tra il diritto comunitario, che, anche per mezzo dei ripetuti interventi della Corte di Giustizia, sta segnando la supremazia della tutela dei dati personali, intesa quale diritto fondamentale, rispetto alle esigenze di sicurezza che, al contrario, appaiono ancora predominanti per il legislatore statunitense e nell'interpretazione del formante giurisprudenziale[25].

Non sorprende, quindi, che nel *draft* dei *Privacy Shield* limitino fortemente la raccolta indiscriminata di dati, che può avvenire in casi estremi e non come normale prassi di sicurezza nazionale[26].

---

invece sostenuta da P. Swire, *US Surveillance Law, Safe Harbor, and Reforms Since 2013*, *Georgia Tech Scheller College of Business Research Paper*, No. #36, secondo cui la convergenza di *rule of law*, separazione dei poteri e controllo giurisdizionale assicurerebbe un livello di protezione sostanzialmente equivalente a quello europeo. L'A. osserva che la Corte di Giustizia non avrebbe considerato adeguatamente le modifiche intervenute nel corso del 2013 e avrebbe valutato non correttamente i mezzi istruttori prodotti durante la controversia.

[23] H.R.1428.

[24] Cfr. D. Bender, *The Judicial Redress Act: A Path to Nowhere, in Privacy Advisor*, Dec. 17, 2015.

[25] In termini simili anche M. Mensi, *Il vero sconfitto è la Commissione europea*, cit., 52, secondo cui «a sopperire le difficoltà della Commissione, la Corte scende in prima linea per rivendicare la primazia di un ordinamento (quello europeo) che, a fronte della *disruptive innovation* della Rete e dei suoi protagonisti (gli operatori Ott, Google, Facebook, Amazon, ecc.), negli ultimi anni aveva segnato il passo a vantaggio di quello di matrice anglosassone, laddove le transazioni online e l'*e-commerce* si sono sviluppate su un sistema più agile e *business friendly*, fondato sull'autodichiarazione e sul consenso delle parti».

[26] Cfr. in particolare il *Considerando 59* dei *Privacy Shield*: «In this regard, the representations of the Office of the Director of National Intelligence (ODNI) provide further assurance that these requirements, including the definition of bulk collection in PPD-28 (n. 5), express a general rule of prioritisation of targeted over bulk collection. According to these representations, Intelligence Community elements «should require that, wherever practicable, collection should be focused on specific foreign intelligence targets or topics through the use of discriminants (e.g. specific facilities, selection terms and identifiers). While PPD-28 explains that Intelligence Community elements must sometimes collect bulk signals intelligence in certain circumstances, for instance in order to identify

3. Corporate Binding Rules

L'azzeramento del *Safe Harbor Agreement* ha imposto un ripensamento degli strumenti giuridici alternativi per il trasferimento transfrontaliero di dati personali, spesso trascurati sia dalla prassi commerciale sia dagli studi dottrinali.

Clausole contrattuali standard e *binding corporate rules* garantiscono la medesima efficacia, legittimando i trasferimenti di dati oltre lo spazio europeo, ma impongono costi transattivi più alti. Quanto appena detto vale specialmente per le clausole contrattuali standard (anche note come *model contract clauses*), che sono clausole da inserire all'interno di contratti tra imprese che non appartengono al medesimo gruppo (cui, invece, sono riservate le *binding corporate rules*)[27].

Le *corporate binding rules* sono, invece, strumenti utilizzati dai gruppi di società per trasferire dati personali da un Paese comunitario o rientrante nello Spazio economico europeo ad un Paese terzo, nel caso in cui il trasferimento avvenga tra società appartenenti allo stesso gruppo. Non si può ricorrere a tale strumento, quindi, quando il soggetto che riceve i dati personali non afferisce al gruppo societario; tale limite vale anche nel caso in cui detto soggetto abbia un rapporto continuativo con la società, titolare del trattamento, che esegue il trasferimento dei dati[28].

Le *corporate binding rules* sono il complesso delle norme tecniche, degli strumenti di sicurezza, delle *policy* aziendali, delle attività di *training* e di *audit* che si intendono realizzare e così via discorrendo, che sono adottate dalle società infragruppo nel trattamento dei dati personali. È necessario il parere positivo di un'autorità garante che, in assenza del consenso del soggetto interessato, legittimi il trasferimento. È altresì richiesto che tale trasferimento sia preventivamente comunicato nell'informativa fornita a clienti e utenti: difatti, sebbene l'autorizzazione del Garante nazionale sia

new or emerging threats, it directs these elements to prioritise alternatives that would allow the conduct of targeted signals intelligence. Hence, bulk collection will only be allowed where targeted collection via the use of discriminants is not possible «due to technical or operational considerations". This applies both to the manner in which signals ntelligence is collected and to what is actually collected. According to representations of the ODNI all this ensures that the exception does not swallow the rule».

[27] Tali costi, poi, sono ancora più alti nel caso in cui si voglia raccogliere il consenso dei singoli soggetti cui si riferiscono i dati personali, atteso che, da un lato, tale pratica impone alle imprese di contattare singolarmente gli interessati e che, dall'altro, la prestazione del consenso potrebbe essere negata dagli stessi.

[28] Cfr. WP 155: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, 2.

finalizzata a scavalcare la necessità della raccolta del consenso, è comunque obbligatorio che il soggetto interessato sia edotto in merito ai soggetti terzi cui potrebbero essere trasferiti i suoi dati personali.

L'*Article 29 Working Party* ha pubblicato numerosi documenti per sensibilizzare le imprese e per fissare le linee guida da seguire nella redazione delle regole imprenditoriali[29]. Si tratta, apparentemente, di regole di *soft-law*, atteso il loro carattere meramente persuasivo e derogabile da parte dei soggetti interessati; tuttavia, l'analisi delle posizioni delle singole Autorità garanti nazionali, che adottano pedissequamente le linee-guida del *Working Party*, induce ad assegnare, seppur di fatto, una natura vincolante a tali regole.

L'Autorità presso la quale presentare la richiesta è quella dove ha sede la società madre ovvero quella della sede societaria presso la quale avviene il trattamento dei dati in via principale[30]. La società scelta deve essere comunque stabilita nell'Unione europea; il *Working Party* elenca i criteri che dovrebbero essere seguiti in tale eventualità, quali, ad esempio, la società che effettuerà il maggior numero di trattamenti di dati, quella che sarà responsabile per le scelte relative alle finalità e alle modalità del trattamento e così via discorrendo[31].

La società che presenterà l'istanza al proprio Garante nazionale sarà altresì responsabile per eventuali violazioni commesse in Paesi terzi; similmente a quanto stabilito per le *standard contract clauses*, è ammessa una

[29] WP 107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From «Binding Corporate Rules»; WP 108: Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules; WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data; WP 153: Working Document setting a table with the elements and principles to be found in Binding Corporate Rules; WP 154: Working Document Setting up a framework for the structure of Binding Corporate Rules; WP 155: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules.

[30] Per la precisione, il Working Party (cfr. WP 108: Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 14 aprile 2005, 3) parla di *«ultimate parent or operational headquarters»*.

[31] Le lingue da utilizzare sono l'inglese e la lingua dell'Autorità nazionale che riceve la richiesta; cfr. WP 133: Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data; nonché WP 107: Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From «Binding Corporate Rules»: «The language of the application shall be set up according to WP 107, Section (8), where [...] as a general rule and without prejudicing to other translations where necessary or required by law, first and consolidated drafts should be provided both in the language of the leading authority and in English. The final draft must be translated into the languages of those DPAs concerned».

responsabilità solidale tra la società esportante e quella importante. In ogni caso, si tratta di previsioni non tassative, nel senso che il gruppo societario può proporre al Garante nazionale una diversa ripartizione delle responsabilità, tenuto conto della propria struttura organizzativa[32].

La Raccomandazione del 2007 stabilisce che la società debba dimostrare che le regole societarie siano approvate internamente (nel senso che vi sia un accordo formale tra la società madre e le società controllate) e quali siano i vantaggi per i soggetti interessati, i cui dati sono trasferiti fuori dai confini europei.

L'art. 43 della proposta di Regolamento ha recepito le istanze del *Working Party*, prevedendo che tutte le società appartenenti al gruppo si impegnino a rispettare i principi previsti in materia di dati personali e, in particolare, i principi di finalità, di minimizzazione dei dati, di conservazione dei dati per periodi limitati, nonché ad adottare le regole di protezione dei dati *by design* e *by default*. Le *corporate binding rules* dovranno inoltre evidenziare le misure per garantire la sicurezza e i principi applicabili a specifiche categorie di dati personali.

Le regole del gruppo dovranno essere approvate secondo il *consistency mechanism* di cui agli artt. 57 ss.: dopo l'approvazione dell'Autorità garante nazionale, sarà richiesto un parere dell'*European Data Protection Board* e (ma il testo della proposta licenziato non è chiaro al riguardo) un'autorizzazione da parte della Commissione.

Le *corporate binding rules* presentano il vantaggio di non incontrare limiti geografici, nel senso che possono essere estese a tutte le società appartenenti al gruppo, anche se vi abbiano aderito successivamente all'approvazione delle regole.

Al contempo, però, sono considerate uno strumento frutto di un processo elaborato e oneroso (i cui tempi sembrano destinati ad allungarsi dopo l'entrata in vigore del Regolamento)[33], che tende a scoraggiare gli interessi imprenditoriali, come dimostra il fatto che solo una ventina di gruppi vi ha fatto sinora ricorso[34]. Inoltre, trovando applicazione ai soli rapporti tra società che appartengono al medesimo gruppo, non possono essere considerate un'alternativa unica agli accordi di adeguatezza, dal

[32] WP 155: Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules, 3.

[33] Al momento, i tempi per ottenere l'autorizzazione sono stimati tra i 18 e i 24 mesi, con una previsione di budget medio di 220.000 dollari, cfr. K. Bloom – K. Royal, *Transferring Personal Data Out of the European Union: Which Export Solution Best Fits Your Needs?*, *Associate of Corporate Counsel*, June 2015, 32 e 34.

[34] K. Bloom – K. Royal, *Transferring Personal Data Out of the European Union*, cit., 30.

momento che, in caso di trasferimento di dati a società terze, si dovrà necessariamente ricorrere ai *model contract clauses*.

4. Model Contract Clauses

Un'ulteriore deroga al generale divieto di trasferimento di dati personali verso Paesi che non assicurino un livello adeguato di protezione è rappresentato, come si diceva, dalle clausole contrattuali standard (o *model contract clauses*, conformemente alla terminologia internazionale). Si tratta di clausole dettate da decisioni della Commissione europea che sono incorporate nel testo dei contratti che regolano l'esportazione di dati personali, contratti a cui aderisce, assumendo specifiche obbligazioni, il soggetto importatore stabilito al di fuori dell'Unione europea.

La fonte normativa, ancora una volta, è il secondo paragrafo dell'art. 26 della Direttiva 95/46/CE: tuttavia, la decisione della Commissione, sebbene non precluda la possibilità che le singole Autorità nazionali rilascino autorizzazioni per il trasferimento dei dati, obbliga le Autorità stesse a riconoscere che le clausole standard, se incluse nei contratti che disciplinano il trasferimento dei dati personali tra un soggetto stabilito nel territorio dell'Unione ed un soggetto extracomunitario, assicurino di per sé un adeguato livello di protezione.

In assenza di accordi di adeguatezza, le *model contract clauses* sono lo strumento maggiormente utilizzato dalle società commerciali per il trasferimento dei dati personali.

Nel momento in cui si scrive, la Commissione europea ha adottato quattro decisioni[35], che, nel corso del tempo, hanno modificato e integrato le clausole inizialmente previste e hanno specificato gli obblighi di esportatori e importatori.

Le *model contract clauses* presentano l'indiscutibile vantaggio di essere

[35] Si tratta della Decisione Commissione, Clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in paesi terzi, dir. 95-46-CE del 5 febbraio 2010; della Decisione della Commissione per l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi del 27 dicembre 2004; della Decisione della Commissione, Clausole contrattuali tipo per trasferimento dati a carattere personale verso paesi terzi a norma dir. 95-46-CE del 5 giugno 2001; della Decisione della Commissione, Clausole contrattuali tipo per trasferimento dati personali a incaricati del trattamento residenti in paesi terzi, dir. 95-46-CE del 27 dicembre 2001.

uno strumento giuridico 'sicuro', nel senso che il loro recepimento legittima l'esportazione dei dati personali verso Paesi terzi che non possono giovare di accordi di adeguatezza. È evidente, tuttavia, che, in quanto clausole da inserire all'interno di un regolamento contrattuale, determinano un aumento dei costi transattivi[36], dal momento che, seppur non modificabili (ma sul punto si ritornerà a breve), si inseriscono all'interno di una negoziazione, gravando l'importatore di una vasta gamma di obblighi e di responsabilità.

Peraltro, è appena il caso di osservare che l'importatore assume tali obblighi – prescritti dalla legge e non frutto di una autonoma manifestazione di volontà – nei confronti sì dell'esportatore, ma nell'interesse del soggetto interessato, che è naturalmente terzo rispetto al contratto stipulato tra le parti[37].

5. L'immodificabilità delle clausole e la soluzione inglese

Le clausole contrattuali standard rappresentano, a parere di chi scrive, un esempio di fonte di integrazione del contratto. Come da tempo ha osservato la migliore dottrina, le fonti di integrazione non operano, infatti, nel solo caso in cui vi siano lacune ovvero dove il regolamento contrattuale sia inidoneo ad operare o sia, in ogni caso, improduttivo di effetti giuridici[38], ma agiscono quali forme di eterointegrazione della volontà contrattuale[39].

Nel caso che ci interessa, tuttavia, la volontà legislativa pare sostitu-

[36] In termini simili anche S.J. Shackelford, *Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations*, in corso di pubblicazione in *Eton Hall J. of Diplomacy & Int'l Rel.* (2016), 4 del dattiloscritto.

[37] Il tema degli obblighi di protezione nel trattamento dei dati personali è affrontato, tra gli altri, da F. Piraino, *Il codice della privacy e la tecnica del bilanciamento di interessi*, in *Libera circolazione e protezione dei dati personali*, a cura di R. Panetta, Milano, 2006, 709 s.

[38] Osserva S. Rodotà, *Le fonti di integrazione del contratto*, Milano, 1969, 8: «il problema dell'integrazione non è strettamente condizionato dall'esistenza di lacune. In altri termini, non è soltanto nei casi di oggettiva inidoneità ad operare del regolamento predisposto dalle parti che può aver luogo il ricorso agli strumenti integrativi (come, invece, continua ad accadere al livello dell'ordinamento legislativo per il ricorso all'analogia)».

[39] S. Rodotà, *op. cit.*, 4.

irsi completamente quella privata[40]. Difatti, se è vero che «gli esportatori e gli importatori dei dati sono pertanto liberi di inserire qualsiasi altra clausola commerciale ritenuta pertinente ai fini del contratto, purché non incompatibile con le clausole tipo», tuttavia la formulazione letterale delle clausole dovrebbe essere lasciata intatta.

Si è in presenza, quindi, di una forma (estrema) rimediale di natura anticipatoria, nel senso che l'ordinamento comunitario si sostituisce all'autonomia dei privati, ritenuti inidonei o incapaci di compiere una valutazione degli interessi in gioco[41]. Non siamo in presenza, quindi, di una clausola da sostituire, perché contraria ad una prescrizione normativa, né, in senso stretto, dinanzi ad una *default rule*[42]. Al più, la fattispecie in esame potrebbe essere accostata alle *immutable rules*, pensate, secondo l'insegnamento della dottrina americana, per tutelare non solo (e non tanto) le parti del contratto, quanto i terzi, la cui sfera giuridica potrebbe essere lesa dagli effetti o dall'esecuzione del contratto stesso[43].

Peraltro, l'ipotesi in esame non rappresenta neanche un caso isolato nella legislazione di derivazione comunitaria: basti pensare, ad esempio, all'art. 129, comma 2 del Codice del consumo, in materia di indici di conformità del bene nella vendita di beni di consumo[44].

La metodologia percorsa dalla Commissione, da un punto di vista comparatistico, appare in antitesi con la visione tradizionale del diritto dei contratti dei sistemi giuridici appartenenti all'area di *civil law*, in cui l'elemento volontaristico è predominante e le forme di sostituzione della volontà privata da parte dell'ordinamento sono considerate come eccezionali[45]. Pertanto, sebbene da tempo si discorra di un avvicinamento della

[40] Intesa, secondo l'insegnamento della migliore dottrina, come libertà di determinare il contenuto del contratto, F. Messineo, *Il contratto in genere*, in *Tratt. dir. civ. e comm.* Dir. da A. Cicu - F. Messineo, Milano, 1966, 802.

[41] Sul punto, per ulteriori rilievi, v. U. Mattei, *I rimedi, in Il diritto soggettivo*, in *Tratt. dir. civile* diretto da R. Sacco, Torino, 2001, 131 ss.

[42] Cfr. V. Roppo, *Il contratto*, Milano, 2011, 435.

[43] In questo senso v. I. Ayres – R. Gertner, *Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, 99 Yale Law Journal* 87 (1989).

[44] L'esempio è menzionato in S. Mazzamuto – A. Plaia, *I rimedi nel diritto privato europeo*, Torino, 2012, 6, cui si rinvia per ulteriori approfondimenti sull'approccio del legislatore comunitario.

[45] Cfr., tra i tanti, G. Mirabelli, *Dei contratti in generale*, in *Comm. Cod. civ.*, IV, t. II, Torino, 1958, 87, e, per l'ordinamento francese, P. Durand, *La tendence à la stabilité du rapport contractuel*, Paris, 1960, 10 ss., ma v. anche, per una comparazione tra Inghilterra e Francia, D. Harris – D. Tallon (eds.), *Contract Law Today: Anglo-French Comparisons,* Oxford, Clarendon Press, 1989.

disciplina contrattuale tra ordinamenti del *common law* e del *civil law*[46], pare plausibile ritenere che l'idea che possa essere il legislatore a fissare i termini del regolamento contrattuale sia mutuato da esperienze appartenenti all'area del diritto angloamericano.

La fattispecie in parola, tuttavia, presenta alcuni elementi peculiari. La Decisione del 2011, all'art. 10, rubricato 'Modifica del contratto', prevede che le parti si impegnino «a non alterare o non modificare le presenti clausole»; è ammesso invece l'inserimento di altre clausole, purché non siano in contrasto con quelle previste dalla Decisione stessa.

Pertanto, dovrebbe concludersi per il divieto assoluto di modificare la formulazione prevista dalla Commissione europea, anche nel caso in cui la stessa sia più favorevole al soggetto interessato.

Una conclusione che risponde, evidentemente, alla necessità, da un lato, per le imprese, di utilizzare un modello contrattuale, appunto, standardizzato e sicuro, in modo da rispondere a criteri di efficienza temporale ed economica. Pare evidente, infatti, che l'eventuale negoziazione singola delle clausole con tutti gli importatori potrebbe determinare aumento dei tempi e dei costi transattivi (*in primis* le spese legali per la revisione dei singoli contratti): in questo modo, inoltre, si risponde anche alla critica, spesso mossa alle clausole contrattuali standard, di non essere estensibili a tutti i rapporti contrattuali dell'impresa con i singoli importatori. Questi ultimi, infatti, sebbene spesso nella pratica degli affari siano soggetti economicamente più deboli e quindi inclini ad aderire acriticamente alle condizioni dell'esportatore, potrebbero non voler assumere specifici obblighi, imponendo alla controparte una negoziazione: eliminare *ab origine* tale rischio si traduce, evidentemente, in un vantaggio per l'impresa esportatrice, che è vincolata, ai sensi del precitato art. 10, al divieto di modifica delle clausole.

Del resto, la modifica delle *model contract clauses* potrebbe determinare altresì l'obbligo di revisione da parte delle Autorità garanti nazionali, che dovrebbero approvare, e conseguentemente autorizzare, le variazioni apportate al testo della Commissione. Anche in questo caso, il divieto di modifica risponde all'esigenza di evitare che le singole Autorità siano gravate da un carico di lavoro eccessivo. Se, poi, si analizza tale ipotesi dalla prospettiva dell'impresa, l'eventuale autorizzazione determinerebbe, inevitabilmente, ulteriori rallentamenti nell'adozione delle stesse, pregiudicando i rapporti commerciali tra esportatore e importatore.

[46] Per tutti, J. Gordley, *The Philosophical Origins of Modern Contract*, Oxford, Clarendon Press, 1991, 1 ss.

Sotto il profilo della patologia del contratto, tuttavia, è bene precisare che la modifica delle condizioni contrattuali non determina, di per sé, alcuna forma di invalidità o di inefficacia del contratto. Al più, come si osservava, pare possibile ipotizzare che l'alterazione della formulazione proposta (*rectius*: imposta) dalla Commissione possa determinare l'insorgere dell'obbligo di ottenere una preventiva autorizzazione da parte dell'Autorità garante competente – che, argomentando *ex* art. 9 della Decisione, è quella del Paese dove è stabilito il soggetto importatore – autorizzazione che legittima il trasferimento dei dati personali al di fuori del territorio dell'Unione europea.

L'assenza dell'autorizzazione, tuttavia, non dovrebbe comportare alcuna forma di responsabilità, né nei confronti dei soggetti interessati né dell'Autorità di garanzia competente. A tale conclusione può pervenirsi argomentando che le clausole, anche se modificate, assicurano comunque uno spettro di tutela adeguato per gli interessati: pertanto, l'eventuale trattamento illecito potrebbe essere al più il frutto di un'indagine specifica del Garante territorialmente competente, nella sola ipotesi in cui gli obblighi assunti dalle parti e dagli eventuali subcontraenti non siano ritenute conformi alle prescrizioni della Commissione europea.

Nel diritto inglese, peraltro, una soluzione parzialmente differente alla questione della modificabilità delle clausole pare essere stata suggerita dall'ICO (*Information Commissioner's Officer*), secondo cui eventuali emendamenti non determinerebbero automaticamente il venir meno del requisito dell'adeguatezza[47]. A giudizio dell'Autorità inglese, infatti, le

[47] ICO, *Model Contract clauses – International transfers of personal data*, 2012, 6: «Use of any version of the model clauses, whether as a stand-alone contract or incorporated into another contract, where the wording is changed (even if the meaning or effect of the changed clause remain unaltered), will not amount to use of clauses that are authorised by the Information Commissioner as providing adequate safeguards under one of the Information Commissioner authorisations set out above. If you choose to amend the model contract clauses, you may take the view that your amended clauses are sufficient to provide adequate safeguards for the protection of the rights of the data subjects whose personal data you propose to transfer. Your amended clauses will not be 'model contract clauses' (attracting the Commission 'guarantee' that they provide adequate safeguards for data subjects rights) but may operate as contractual arrangements which in the reasonable view of the data controller provide adequate safeguards for data subjects' rights. Providing adequate safeguards by using your own clauses is an equally valid basis on which to proceed with a transfer as is the use of model contract clauses. The only difference is that you need to be prepared to offer evidence in support of your view (that your clauses provide adequate safeguards) if it is challenged. If you use model contract clauses, given that the Commission has determined that such clauses offer adequate safeguards, there can be no challenge as to the effectiveness of the safeguards the model contract

variazioni al testo approvato dalla Commissione europea comporterebbero solo l'insorgere, in capo all'esportatore dei dati personali, dell'onere di dover dimostrare che le nuove clausole siano idonee ad assicurare un livello di protezione pari a quello previsto dalle decisioni comunitarie.

Si deve ritenere, quindi, che, a giudizio del Garante inglese, tale controllo sia successivo ed eventuale e che, quindi, non sia richiesta neanche un'autorizzazione preventiva da parte dell'autorità nazionale alla modifica delle clausole. Tale conclusione, del resto, risponde sia ad un'ottica solidaristica e antiformalistica della tutela dei soggetti interessati, sia ad un'ottica giuseconomica, considerando i costi transattivi associati alla riscrittura delle clausole contrattuali.

Difatti, da un lato la modifica delle clausole, nel caso in cui siano apprestate comunque garanzie adeguate o addirittura superiori (ad esempio, l'adozione di specifiche misure di sicurezze per la protezione dei dati) rispetto a quelle dettate dalla Commissione, risponde alle esigenze di tutela non solo delle controparti contrattuali, ma anche (e soprattutto) dei soggetti terzi (ossia dei soggetti cui appartengono i dati personali). Dall'altro, se la variazione del testo delle clausole richiedesse l'autorizzazione preventiva dell'Autorità garante nazionale, allora sarebbe una soluzione in gran parte impraticabile, dal momento che causerebbe un significativo aumento dei tempi per l'approvazione del contratto e un aumento, altrettanto significativo, dei costi transattivi relativi al contratto stesso.

La scarsa flessibilità delle *standard contractual clauses*, del resto, aveva indotto la Commissione ad adottare una Decisione nella quale, alle originarie clausole del 2001, erano affiancate clausole alternative e differenti, proposte e negoziate da un consorzio di associazioni imprenditoriali[48].

Tale decisione, però, a proposito dell'annosa questione di cui si discute, aveva fornito una risposta negativa, emendando l'art. 1 della Decisione 2001/497/CE e stabilendo (in anticipo rispetto alla Decisione del 2011) il divieto di modifica o di combinare le clausole della Decisione del 2001 con quelle del 2004.

clauses offer».

[48] Cfr. Decisione della Commissione per l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi del 27 dicembre 2004, *Considerando n. 2*. Il consorzio era formato da: Camera di commercio internazionale (ICC), Japan Business Council in Europe (JBCE), European Information and Communications Tech- nology Association (EICTA), EU Committee of the American Cham- ber of Commerce in Belgium (Amcham), Confederation of British Industry (CBI), International Communication Round Table (ICRT) e Federation of European Direct Marketing Associations (FEDMA).

Aderendo all'interpretazione più restrittiva, considerando quindi immodificabili le clausole, dovrebbe peraltro ritenersi che il contratto possa essere stipulato esclusivamente in una delle lingue dell'Unione europea (lingue nelle quali le *standard contract clauses* sono disponibili) e che l'eventuale traduzione nella lingua madre dell'importatore, costituendo in ogni caso una variazione rispetto al testo licenziato dalla Commissione, non possa essere la lingua del contratto avente ad oggetto il trasferimento dei dati personali[49].

6. Rapporti tra importatore ed esportatore

Un altro dei punti critici della clausole contrattuali standard è rappresentato dalla rigidità dei rapporti tra importatore ed esportatore e dalle complessità associate ad eventuali subcontratti.

Ai sensi dell'art. 3 della Decisione del 2011, l'esportatore è qualificato quale titolare del trattamento (ovvero come responsabile, conformemente alla terminologia comunitaria), mentre l'importatore riveste il ruolo di incaricato del trattamento. La Decisione, quindi, esclude la possibile sussistenza di una contitolarità nel trattamento dei dati tra i due soggetti, conformemente a quanto previsto da alcune decisioni dei Garanti nazio-

[49] Così K. Bloom – K. Royal, *Transferring Personal Data Out of the European Union*, cit., 32. Gli studi di diritto comparato hanno evidenziato le insidie nella traduzione dei termini giuridici e la frequenza con cui termini apparentemente simili celino concetti giuridici differenti: tra i tanti studi sulla materia si rinvia a R. Sacco, *Riflessioni di un giurista sulla lingua (la lingua del diritto uniforme, e il diritto al servizio di una lingua uniforme)*, in *Riv. dir. civ.*, 1996, I, 57, Id., *Traduzione giuridica*, in *Dig. disc. priv., sez. civ.*, Agg., 2000, 722; L.-J. Constantinesco, *Il metodo comparativo,* ed. it. a cura di A. Procida Mirabelli di Lauro, Torino, 2000, 123; M. Morris (ed.), *Translation and the Law*, in *American Translators Association Scholarly Monograph Series*, VIII, Amsterdam-Philadelphia, 1995; B. Pozzo (a cura di), *Lingua e diritto: oltre l'Europa*, Milano, 2014; C.J.W. Baaij *The Role of Legal Translation in Legal Harmonization*, Kluwer Law Int., 2014; S. *Šarčević*, *Language and Culture in EU Law. Multidisciplinary Perspectives*, Ashgate, 2015. Nella prassi dei contratti aventi ad oggetto il trasferimento di dati personali, il linguaggio e la terminologia, anche a livello internazionale, sono generalmente mutuati da quelli delle normative comunitarie, dalle quali sono riprese le definizioni e la ripartizione dei soggetti coinvolti (es. soggetto interessato, titolare/responsabile del trattamento, incaricato, ecc.); ciò tuttavia non esclude a priori l'eventualità di errori, *false friends* e ulteriori imprecisioni, determinati dalle diversità tra gli istituti giuridici nazionali (basti pensare alla panoplia dei rimedi apprestati dai singoli ordinamenti giuridici in caso di violazione degli obblighi contrattuali).

nali[50], nonché l'eventualità che l'importatore sia tenuto a trattare i dati personali ricevuti «per conto e secondo le istruzioni dell'esportatore stesso», permanendo in capo a quest'ultimo la titolarità (e, pertanto, il potere di determinare gli strumenti, le modalità e le finalità del trattamento).

È ammesso il subcontratto ossia l'eventualità che l'importatore assegni a terzi l'esecuzione, totale o parziale, degli eventuali obblighi assunti nei confronti dell'esportatore; in questa ipotesi, è però richiesto il previo consenso scritto dell'esportatore (clausola 11). A fronte di un subcontratto, tuttavia, l'importatore resterà responsabile, in via solidale, nei confronti dell'esportatore e del soggetto interessato, per gli eventuali obblighi di protezione previsti dall'accordo stipulato con l'esportatore.

Il regime di responsabilità delineato dalla Decisione del 2010 presenta alcune singolarità, se comparato a quello della direttiva 95/46/CE[51], sebbene esso sia, essenzialmente e nei termini in cui si dirà a breve, di natura mista (vicaria e sussidiaria).

La clausola 6 della Decisione del 2011, infatti, stabilisce che l'interessato che abbia subito un danno che sia riconducibile alla condotta di una delle parti del contratto di trasferimento dati ovvero a quella del subincaricato, abbia «diritto di ottenere dall'esportatore il risarcimento del danno sofferto».

In prima istanza, quindi, la Commissione europea ha scelto di imputare all'importatore il costo degli eventuali illeciti trattamenti dei dati per-

[50] Cfr. ICO, *Guide to Data Protection. Sending personal data outside the European Economic Area (Principle 8)*, nonché Garante per la protezione dei dati personali, provv. 15 giugno 2011, *Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali*, in *Gazz. Uff.*, n. 153 del 4 luglio 2011, in cui l'Autorità ha chiarito che i call center non possano essere nominati contitolari del trattamento, ma che la titolarità debba rimanere in capo al soggetto che stabilisce le modalità e le finalità del trattamento dei dati personali.

[51] Sul modello di responsabilità civile previsto dalla direttiva si rinvia, *ex multis*, a S. Sica, *Commento sub art. 18*, in E. Giannantonio - M. G. Losano - V. Zeno- Zencovich, *La tutela dei dati personali. Commentario alla l. 675/96*, Padova, 1997, 176 ss.; M. Franzoni, *Dati personali e responsabilità civile*, in *Resp. civ. prev.*, 1998, 902 ss.; G. Comandè, *Danni cagionati per effetto del trattamento dei dati personali*, in F.D. Busnelli - C.M. Bianca, *Tutela della privacy*, in *Nuove leggi civ. comm.*, 1999, 482 ss.; F.D. Busnelli, *Il «trattamento dei dati personali» nella vicenda dei diritti della persona: la tutela risarcitoria*, in V. Cuffaro - V. Ricciuto - V. Zeno-Zencovich, *Trattamento dei dati e tutela della persona*, Milano, 1998, 177 ss.; G. Alpa, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. Inf.* 1997, 703 ss.; D. Carusi, *La responsabilità*, in V. Cuffaro - V. Ricciuto, *Il trattamento dei dati personali*, 2a ed., Torino, 1999, 356 ss.; G. Buttarelli, *Banche dati e tutela della riservatezza*, Milano, 1997, 350 ss.; V. Roppo, *La responsabilità civile per trattamento di dati personali*, in *Danno e resp.*, 1997, 660 ss.

sonali, così come avviene all'interno della direttiva, che prevede la responsabilità del titolare del trattamento anche per il fatto degli incaricati. Una opzione normativa che risponde ad almeno due esigenze: da un lato, quella di favorire la posizione processuale dell'interessato, che non sarà costretto ad indirizzare la propria richiesta risarcitoria ad un soggetto stabilito fuori dai confini dell'Unione europea e, dall'atro, quella di allocare i *costs of accidents* in capo all'importatore che, nella maggior parte dei casi, è la *deep pocket party*, ossia il soggetto economicamente nella posizione più efficiente per compensare i costi del risarcimento dovuto all'interessato[52].

La Decisione del 2010 prende in esame anche la fattispecie in cui l'esportatore sia «scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente»: in questa eventualità, la responsabilità si trasferirà in prima istanza sull'importatore, che sarà chiamato a rispondere anche delle violazioni commesse dall'importatore nonché, a titolo solidale, di quelle commesse dal subincaricato, non potendo eccepire la violazione degli obblighi assunti da quest'ultimo «al fine di escludere la propria responsabilità», come espressamente disposto dalla clausola 6, secondo capoverso.

La responsabilità del subincaricato è, al pari di quella dell'importatore, di natura sussidiaria, atteso che l'interessato potrà rivalersi in giudizio nei suoi confronti nel solo caso in cui sia l'importatore sia l'esportatore «siano scomparsi di fatto, abbiano giuridicamente cessato di esistere o siano divenuti insolventi» (clausola 6, terzo capoverso). Il subincaricato, tuttavia, risponderà esclusivamente per i trattamenti effettuati da quest'ultimo e non anche per quelli posti in essere esclusivamente dall'importatore o dall'esportatore.

In entrambe le fattispecie descritte, il meccanismo della sussidiarietà agirà esclusivamente laddove non vi sia una successione nei rapporti giuridici dell'esportatore o dell'importatore e gli obblighi contrattuali non siano stati trasferiti ad altro soggetto, per contratto o per legge.

La tutela apprestata a favore dell'interessato è poi rafforzata dalla clausola 7, relativa a mediazione e giurisdizione. In base a tale clausola, l'importatore si impegna, in caso di azione per il risarcimento del danno,

[52] Per tutti, G. Calabresi, *Costo degli incidenti e responsabilità civile*, trad. a cura di A. De Vita - V. Varano - V. Vigoriti, pref. di S. Rodotà, Milano, 1975, 65 ss.; l'A. definisce l'allocazione dei costi sui soggetti con maggiori capacità patrimoniali come il metodo più adatto a «ridurre i costi secondari dei sinistri» trasferendoli «su quelle categorie di persone, la cui posizione sociale ed economica meno ne risentirebbe, su quelli, cioè, che generalmente si sogliono definire 'ricchi'»; ma similmente anche R. Posner, *Strict Liability: A Comment*, 2 *J. Legal Studies* 205, 210 (1973).

a «sottoporre la controversia alla mediazione di un terzo indipendente o eventualmente dell'autorità di controllo» ovvero a «deferire la controversia agli organi giurisdizionali dello Stato membro in cui è stabilito l'esportatore».

La Commissione, però, nella consapevolezza che, nell'economia globalizzata, spesso i soggetti interessati possono essere residenti in un Paese diverso rispetto a quello dell'esportatore, fa salvi i «rimedi giuridici previsti dalla normativa nazionale o internazionale»: in altri termini, l'interessato potrà beneficiare delle norme di diritto internazionale privato in materia di illecito aquiliano che stabiliscono l'applicabilità del foro competente dell'attore e della legge applicabile del luogo in cui si sono manifestati gli effetti dannosi della condotta illecita.

Conclusioni

Sino alla sentenza Schrems, *standard contractual clauses* e *corporate binding rules* hanno rivestito un ruolo ancillare rispetto ai *safe harbor agreement* e, in generale, agli accordi di adeguatezza per una molteplicità di ragioni, alcune delle quali sono già state esposte in precedenza.

Innanzi tutto, perché il *safe harbor agreement* è stato considerato uno strumento più sicuro, anche per i controlli blandi esercitati da parte della *Federal Trade Commission* sull'adempimento degli accordi da parte delle società aderenti[53], controlli che, già prima dell'intervento della Corte di Giustizia, avevano sollevato non poche critiche da parte della Commissione[54].

L'inefficiente esercizio della funzione deterrente pare accomunare,

[53] La FTC è intervenuta meno di 20 volte per sanzionare la violazione degli accordi di *Safe Harbor* (e, in dodici casi, si è giunti ad una mediazione con i soggetti coinvolti sul pagamento delle relative sanzioni). Peraltro, la maggior parte degli interventi dell'Autorità statunitense sono avvenuti nel corso del 2014, dopo gli interventi della Commissione europea, cfr. K. Bloom – K. Royal, *Transferring Personal Data Out of the European Union*, cit., 36.

[54] Cfr. Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, 27.11.2013; Communication from the Commission to the European Parliament and the Council, *Restoring Trust in EU-US data flows*, COM(2013) 846 final, 27.11.2013, nonché il relativo Memorandum *Restoring Trust in EU-US data flows – Frequently Asked Questions*, MEMO/13/1059, 27.11.2013.

invero, gli accordi di adeguatezza (e, in special modo, quelli di *safe harbor*) e i modelli contrattuali standard, sottolineando la natura formalistica della legislazione in materia di protezione dei dati personali[55]. In altri termini, occorre domandarsi se la predisposizione di modelli contrattuali standard ovvero, per le imprese legittimate, delle *corporate binding rules* siano effettivamente in grado di tutelare i diritti dei soggetti interessati o se si riducano, nei fatti, all'adesione formalistica alle prescrizioni derivanti dalla normativa o ordinate dalle Autorità Garanti.

Di là da tali rilievi, preme osservare che le alternative agli accordi di adeguatezza presentano non pochi svantaggi, alcuni dei quali sono già stati menzionati nelle precedenti pagine.

Le *standard contractual clauses* sono tendenzialmente anelastiche, non potendo essere modificate dalle parti del contratto, e impongono dei limiti così stringenti in caso di subcontratto da non poter trovare applicazione ad alcune tipologie di contratti (es. contratti aventi ad oggetto i servizi di *cloud computing*) in cui il trasferimento dei dati personali è connaturato alla natura stessa del contratto.

Le *corporate binding rules*, d'altro canto, incontrano il limite della loro applicabilità esclusivamente ai trasferimenti di dati personali tra società del medesimo gruppo, non potendo essere estese ai rapporti con società terze. Peraltro, la necessità di una preventiva autorizzazione da parte dell'Autorità Garante determina una significativa espansione dei tempi, spesso difficilmente conciliabile con la rapidità dei traffici commerciali, e la necessità di redigere tali regole per il gruppo societario, in maniera analitica, destinando risorse umane a tale compito e ai rapporti con l'Autorità Garante.

Alla luce di tali riscontri, non può concludersi che, sebbene siano, sul piano dell'efficacia, alternativi ai *safe harbor*, legittimando gli scambi di dati personali tra Europa e Stati Uniti, *corporate binding rules* e *model contract clauses* non rappresentano dispositivi normativi in grado di fronteggiare l'alluvione scaturita dalla sentenza della Corte di Giustizia. Un'alluvione che è stata determinata dall'azzeramento immediato dell'originario *safe harbor agreement*, a partire dal momento della pubblicazione della sentenza, come precisato dal *Working Party* e dai Garanti nazionali[56].

[55] Sul punto, per più ampi rilievi, si rinvia a S. Sica, *Art. 1350. Degli atti che devono farsi per iscritto*, in *Comm. cod. civ.* diretto da F.D. Busnelli, Milano, 2003, 276 ss., che discorre, a proposito degli adempimenti richiesti dalla normativa privacy, di neoformalismo procedimentale.

[56] Cfr. lo *Statement* dell'Article 29 Working Party, 16 October 2015, 2; Garante per la protezione dei dati personali, provv. 22 ottobre 2015, *Trasferimento dati personali verso gli*

Le imprese si trovano – almeno fino al varo definitivo del *Privacy Shield* – a doversi raffrontare con un vuoto normativo che pregiudica il loro operato e che, teoricamente, rischia di paralizzare (o, quanto meno, di ritardare) i traffici commerciali tra Europa e Stati Uniti. Sebbene le istanze di tutela recepite dalla Corte di Giustizia appaiano assolutamente condivisibili e sebbene non si possa non rimarcare il lassismo, probabilmente voluto, degli Stati Uniti, che non hanno saputo fronteggiare adeguatamente l'emergenza PRISM e non hanno voluto ripensare il loro modello di sorveglianza massiva, non può non concludersi per la complessiva inadeguatezza degli strumenti alternativi sopravvissuti alla decisone dei giudici comunitari. Tali strumenti, difatti, non appaiono in grado di tamponare la mole degli scambi intercontinentali di dati personali e di supplire, neanche temporaneamente, al vuoto lasciato dall'annullamento dei *safe harbor*.

Abstract

The ECJ's ruling Schrems v. Data Protection Commissioner *has invalidated the EU-US Safe Harbor Agreement. The decision is the third step of the European Court of Justice – after the* Digital Ireland *and* Costeja Gonzales *cases – towards the acknowledgment of personal data protection as a fundamental right, pursuant to article 9 of the Treaty of Nice, and marks the rift between EU and US on the fair balance among surveillance systems and privacy laws. After the collapse of the Safe Harbor Agreement and before the implementation of the so-called Privacy Shield, binding corporate rules, for multinational organizations or groups of companies, and contract model clauses, in any other case, have been the sole compliant solutions for overseas transfers of personal data.*

USA: caducazione provvedimento del Garante del 10.10.2001 di riconoscimento dell'accordo sul c.d. «Safe Harbor», in *Gazz. Uff.*, n. 271 del 20 novembre 2015.

Alessandro Mantelero

I flussi di dati transfrontalieri e le scelte delle imprese tra Safe Harbour *e* Privacy Shield

Sommario: Premessa. La *ratio* del «Safe Harbour» ed il suo vizio d'origine. – 1 Il post «Safe Harbour». Strategia di breve periodo. – 1.1 (*segue*). Strategia di medio periodo. – 1.2 (*segue*). Strategia di lungo periodo e valore competitivo della tutela dei dati personali. – 2. Prime conclusioni. – 3. «Privacy Shield». Quasi un epilogo

Premessa. La ratio del Safe Harbour *ed il suo vizio d'origine*

La sentenza della Corte di Giustizia dell'Unione europea sul caso Schrems[1] ha posto fine ad un compromesso, il «Safe Harbour», frutto di un'intesa politica fra Stati Uniti ed Unione europea. Non è infatti possibile ridurre il «Safe Harbour» ad un semplice programma di autocertificazione[2] adottato dal governo statunitense (Department of Commerce) al fine di individuare le imprese che si impegnavano ad offrire uno standard di tutela ritenuto dalla Commissione Europea adeguato ai sensi dell'art. 25, dir. 95/46/CE.[3] Una tale formale ed anonima costruzione, incentrata sul

[1] Cfr. Corte di Giustizia dell'Unione europea, 6 ottobre 2015, C-362/14, *Maximillian Schrems v Data Protection Commissioner, Digital Rights Ireland Ltd*, http://curia.europa.eu/juris/liste.jsf?num=C-362/14. Ad eccezione del paragrafo 3, tutti i link ipertestuali a cui è fatto rinvio nelle presenti note sono riferiti a contenuti disponibili *online* e visionati in data anteriore al 15 novembre 2015.

[2] Cfr. European Commission, *Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, 2000/520/EC (in seguito European Commission, 2000/520/EC), Annex I e Annex II, FAQ n. 6.

[3] Con riguardo alla nozione di 'adeguatezza', la Corte precisa che «The word 'adequate' in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term 'adequate level of protection' must be understood as requiring the third country in fact to

giudizio di adeguatezza, cela infatti le reali ragioni dell'accordo, ragioni che ne hanno incisivamente influenzato i contenuti.

Per comprendere l'effettiva portata giuridica e le conseguenze della decisione che ha invalidato il «Safe Harbour» e per delineare i possibili scenari futuri, occorre dunque adottare una prospettiva più ampia, superando una visione parcellizzata ed atomistica dei fenomeni giuridici. Serve quindi partire dalle origini, ovvero dai motivi che portarono all'accordo con gli Stati Uniti e dalla natura eccezionale dello stesso.[4] Perché lì risiede la *ratio* dell'anomalia che ha indotto la Corte di Giustizia alla dichiarazione d'invalidità, stante la natura genetica del vizio.

I giudici di Lussemburgo hanno rilevato come la Commissione Europea, chiamata a valutare il livello di tutela offerto dalla normativa statunitense in termini di protezione dei dati, non abbia di fatto tenuto conto del quadro regolamentare, sostituendo l'adeguatezza dello strumento («Safe Harbour»)[5] all'adeguatezza dell'ordinamento statunitense, creando un *tertium genus* non previsto dagli artt. 25 e 26 della direttiva. Tali norme delineano infatti solamente due modalità volte a garantire un livello adeguato di protezione dei dati: l'accordo fra *data importer* e *data exporter* o l'esistenza nel Paese terzo di un ordinamento giuridico che offra tale livello di protezione.[6]

La Commissione sembra dunque aver ravvisato nel «Safe Harbour» una sorta di accordo quadro fra imprese statunitensi ed europee, non è

ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter».

[4] Si vedano in proposito le considerazioni espresse da G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE* e da S. Sica e V. D'Antonio, *I Safe Harbour Privacy Principles: genesi, contenuti, criticità*, entrambi in questo Volume.

[5] Cfr. European Commission, 2000/520/EC, cit., considerando n. 5 nel preambolo della decisione ed art. 1.

[6] Nello specifico, ai sensi dell'art. 25(6) dir. 95/746/EC, la Commissione può valutare che il livello di protezione offerto dal Paese terzo sia adeguato anche in ragione «of the international commitments it has entered into», per cui il «Safe Harbour» poteva astrattamente costituire lo strumento per garantire l'adeguatezza. Il vizio, che ha portato all'invalidità dell'accordo in questione, sta però nel fatto che l'adeguatezza è stata riconosciuta sulla base della sola adesione al «Safe Harbour», senza considerare che tale accordo prevedeva ampie deroghe a favore della legislazione statunitense, in virtù delle quali quest'ultima prevaleva sugli obblighi imposti dall'accordo alle imprese aderenti. Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punti 83-84. In conseguenza di ciò, un giudizio corretto sull'adeguatezza della tutela offerta ai dati negli USA avrebbe dovuto tenere conto anche delle disposizioni vigenti, per la parte in cui prevalevano sull'accordo «Safe Harbour». Cfr. anche i successivi punti 87-88 e 96-97.

tuttavia questa la natura del «Safe Harbour». Occorre dunque chiedersi quali ragioni hanno indotto la Commissione a travisare consapevolmente il disposto dell'art. 26 e come sia stato possibile che per tre lustri un sistema ampio e complesso di flussi transfrontalieri si sia retto su un accordo illegittimo, senza alcuna sospensione o revoca dello stesso.[7]

In questi anni molte voci critiche si sono levate contro il «Safe Harbour», sostanzialmente in quanto la nozione di 'porto sicuro' appariva più un salvacondotto agevolmente rilasciato alle imprese statunitensi,[8] che

[7] Non sono mancate, in tempi recenti, prese di posizione critiche da parte delle istituzioni comunitarie, cfr. European Commission, *Communication from the Commission to the European Parliament and the Council. Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 final, Brussels, 27 novembre 2013; European Commission, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, Brussels, 27 novembre 2013, COM(2013) 847 final. Cfr. anche European Parliament, *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, Strasburgo, 12 marzo 2014, P7_TA(2014)0230, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139. Nessuna di tale azione si è tuttavia tradotta in una sospensione dell'accordo, ma solamente le istituzioni comunitarie si sono adoperate per una rinegoziazione dello stesso. La sospensione dell'accordo è stata tuttavia richiesta dalla Commissione Civil Liberties, Justice and Home Affairs del Parlamento Europeo, cfr. LIBE Committee, *NSA snooping: MEPs table proposals to protect EU citizens' privacy Fundamental rights*, Press release 12 febbraio 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20140210IPR35501%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN. In merito all'impatto dei programmi di sorveglianza di massa statunitensi sulla dialettica fra Unione europea e Stati Uniti con riguardo al trattamento transfrontaliero di dati, si rinvia all'analisi svolta da G. Resta, *La sorveglianza di massa e il conflitto regolatorio USA/UE*, cit.

[8] Cfr. C. Connolly, *EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance. Speaking/background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on «Electronic mass surveillance of EU citizens»*, Strasburgo, 7 ottobre 2013, http://www.europarl.europa.eu/document/activities/cont/201310/20131008ATT72504/20131008ATT72504EN.pdf. Cfr. anche le dichiarazioni rilasciate da Jeff Chester, executive director del Center for Digital Democracy, in J. Chester, *CDD Files Complaint on U.S./EU Safe Harbor for Data Privacy at FTC/ Filing Reveals Failure of U.S. Agreement to Protect European Privacy*, Center for Digital Democracy, 14 agosto 2014. https://www.democraticmedia.org/content/cdd-files-complaint-useu-safe-harbor-data-privacy-ftc-filing-reveals-failure-us-agreement («Instead of ensuring that the U.S. lives up to its commitment to protect EU consumers, our investigation found that there is little oversight and enforcement by the FTC. The Big Data-driven companies in our complaint use Safe Harbor as a shield to further their information-gathering practices

una garanzia per i cittadini europei circa il trattamento dei propri dati oltreoceano.[9] I princìpi del «Safe Harbour»,[10] cui le imprese statunitensi dovevano aderire per ricevere informazioni personali dall'EEA senza dover porre in essere adempimenti ulteriori, erano già in sé una 'riduzione' delle disposizioni chiave della normativa comunitaria in materia. A ciò si aggiunga una prassi in cui molte delle imprese aderenti al «Safe Harbour» non risultavano di fatto nemmeno conformarsi ai requisiti richiesti dall'accordo stesso.[11]

Sino a qui dunque, e per sommi capi, i caratteri distintivi dell'accordo; per cogliere le ragioni dell'anomalia del «Safe Harbour» occorre però guardare altrove, al disposto dell'art. 25 della dir. 95/46/CE ed alla *ratio* ispiratrice di tale disposizione. La logica sottostante risiede nell'intento di non vanificare gli sforzi posti in essere dagli Stati europei nel dotarsi di uno standard in gran parte uniforme in materia di protezione dei dati personali, attestato su un livello di più elevato di quello offerto dagli altri modelli esistenti.[12]

Creata, non senza difficoltà, questa comune area di circolazione sicura dei dati, in termini di tutela offerta, l'Unione europea non poteva veder vanificata la propria opera ammettendo che processi di delocalizzazione delle risorse informative potessero sottrarre i dati personali alla disciplina comunitaria. La ragione ultima delle dinamiche che hanno portato al

without serious scrutiny. Companies are relying on exceedingly brief, vague, or obtuse descriptions of their data collection practices, even though Safe Harbor requires meaningful transparency and candor. Our investigation found that many of the companies are involved with a web of powerful multiple data broker partners who, unknown to the EU public, pool their data on individuals so they can be profiled and targeted online»). Meno critici a riguardo S. Sica e V. D'Antonio, *I Safe Harbour Privacy Principles: genesi, contenuti, criticità*, cit., i quali rilevano come i Safe Harbour Principles abbiano rappresentato «una sorta di by-pass tra la tutela dei dati personali di stampo comunitario e il diverso approccio adottato negli Stati Uniti».

[9] Cfr. Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, 14 October 2015, punto 4, https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,-C-36214.html («the CJEU argued that the Commission did not make any statement about the level of data protection in the US, but instead chose with the Safe Harbour principles, an inapt construction as compensation for an inadequate level of protection»).

[10] Per una disamina di tali principi si rinvia a S. Sica e V. D'Antonio, *I «Safe Harbour» Privacy Principles: genesi, contenuti, criticità*, cit.

[11] Cfr. supra n. 5 e 6.

[12] Cfr. anche Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 73.

«Safe Harbour» risiede dunque nella tensione cui è sottoposta la nozione di territorialità del diritto in relazione alle tecnologie digitali ed alla diffusione delle reti elettroniche di comunicazione.[13]

Abbandonati i dati cartacei e l'età dei *mainframe*, in cui per ragioni diverse lo spostamento di banche dati da un luogo all'altro risultava non solo complesso, ma anche facilmente monitorabile, nell'era della rete internet in cui terabyte di dati possono fluire agevolmente da un qualsiasi computer di un cittadino europeo verso qualsiasi punto del globo, appare estremamente fragile l'idea di creare mura a difesa dei propri standard di protezione. Non a caso la stessa Cina, che molto ha investito nella protezione dei propri confini informatici sia in termini tecnologici che normativi, conosce non pochi casi di aggiramento del proprio sistema.

Come potevano dunque gli stati europei pensare di aver successo in una simile opera 'difensiva', seppur animata dall'intento di offrire maggior tutela ad un diritto fondamentale? La chiave di volta del modello europeo, che ne ha segnato l'indubbio successo in termini di circolazione e recezione ad opera di Paesi terzi,[14] non è stata né la forza politica, né quella tecnologica, bensì quella economica, intesa non come forza intrinseca delle imprese europee, bensì come sfruttamento dei legami di interdipendenza esistenti in un contesto di economia globalizzata.

Non i Paesi terzi, bensì le imprese europee sono state nel contempo il *target* e gli alfieri della diffusione del modello europeo. Ponendo la regola secondo cui i dati personali non possono essere inviati al di fuori dell'EEA verso Paesi che non offrano adeguati livelli di tutela,[15] si è in concreto fatto leva sulla dipendenza reciproca esistente fra imprese commerciali europee ed imprese dei Paesi terzi, in un contesto di economia dell'informazione.

Come dimostrato *ex post* dalle reazioni che hanno fatto seguito alla decisione della Corte di Giustizia, il valore assunto dai dati in tutti gli aspetti della vita economica ha reso impensabile che, da un lato, le imprese europee potessero decidere di circoscrivere la loro operatività entro i confini dello spazio economico europeo che, d'altro canto, che, per non

[13] Cfr. in proposito la più ampia disamina sul rapporto fra regolamentazione e sovranità digitale nelle reti globali elaborata da V. Zeno-Zencovich, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione*, in questo Fascicolo.

[14] Cfr. G. Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, in International Data Privacy Law*, 2012, 2(2), 68 ss.; G. Greenleaf, *Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority, in Privacy Laws & Business International Report*, 2015, 133.

[15] Cfr. art. 25 dir. 95/46/CE.

adempiere alle norme in materia di *data protection*, i *partners* commerciali delle imprese europee decidessero di rinunciare agli accordi negoziali in essere con esse.

Non solo, sotto il profilo organizzativo, una volta che le suddette ragioni hanno indotto le imprese dei Paesi terzi ad adottare standard simili a quelli comunitari, si è in molti casi generata una sorta di propagazione spontanea di questi ultimi. In un contesto dominato dall'elaborazione aggregata delle informazioni originate da fonti diverse, è risultato infatti sovente impossibile od inefficiente, per i *partners* degli operatori comunitari, separare i dati provenienti da questi ultimi dai dati propri.

Infine, gli stati stessi, spesso a ciò indotti dalle proprie imprese, hanno ritenuto vantaggioso adottare delle norme in materia di *data protection* che fossero conformi al modello comunitario, onde ridurre gli oneri in capo alle imprese locali in termini di negoziazione ed adeguamento al livello di tutela richiesto dall'Unione.[16]

Una simile forma di circolazione del modello europeo, incentrata sulle dinamiche proprie delle relazioni commerciali, non poteva di certo operare pienamente nei confronti dell'attuale maggiore potenza economica ovvero gli USA. Questo non solo in ragione della forza delle società nordamericane, ma soprattutto in conseguenza della forza politica del governo e delle istituzioni statunitensi.

In quest'ottica, il «Safe Harbour» viene alla luce come compromesso, come soluzione figlia di accordi politici. L'accordo in questione viene poi accolto favorevolmente da parte degli operatori economici di entrambe le sponde dell'Atlantico, essendo ancora lontana una cultura diffusa della *data protection* come valore di impresa e fattore competitivo, prevalendo invece una lettura che ravvisa nella tutela dei dati una mera voce di costo.

[16] Si veda in proposito il caso emblematico dell'India e dell'interesse all'adozione di un modello simile a quello europeo al fine di attrarre la delocalizzazione dei servizi di outsourcing informatico, su cui volendo A. Mantelero, *La nuova normativa indiana in materia di* data protection*: la protezione dei dati declinata in maniera funzionale all'*outsourcing, in *Contratto e impr. Europa*, 2011, 728 ss. Cfr. anche G. Greenleaf, *Promises and illusions of data protection in Indian law*, in *International Data Privacy Law*, 2011, 1 (1), 47 ss.

1. Il post «Safe Harbour». Strategia di breve periodo

Se questi sono gli antecedenti storici della situazione attuale, occorre chiedersi quali siano le attese per il futuro in termini di tutela delle informazioni provenienti dall'Unione europea ove trattate dalle imprese statunitensi. A tal proposito pare opportuno distinguere fra scenari e soluzioni giuridiche di breve, medio e lungo periodo. Questo poiché le prospettive di un nuovo accordo, come gli strumenti legali per legittimare il flusso transfrontaliero di dati, hanno tempi di realizzazione ed oneri variabili, ragion per cui è immaginabile che gli operatori economici possano elaborare scelte differenziate nel tempo, anche in ragione della loro dimensione organizzativa e della natura e complessità dei flussi transfrontalieri cui danno origine.

Va in primo luogo rilevato come l'invalidità del «Safe Harbour» non escluda, in teoria, un giudizio positivo sull'adeguatezza della tutela offerta dall'ordinamento statunitense, tanto è vero che sul punto, a seguito della decisione della High Court irlandese successiva al rinvio pregiudiziale,[17] spetterà al garante irlandese pronunciarsi sul caso posto all'esame dei giudici lussemburghesi e valutare se il flusso transfrontaliero verso gli USA originato da Facebook sia tale da esporre i dati dei cittadini europei ai rischi derivanti da un livello di tutela che non sia «essentially equivalent» a quello goduto nell'Unione.

Poiché tuttavia nella pronuncia della Corte di Giustizia sono già presenti molti indici per concludere in senso negativo suddetta valutazione, ben si spiega come sin da subito la macchina politica si sia mossa su entrambe le sponde dell'Atlantico al fine di raggiungere quanto prima una nuova soluzione compromissoria basata su un accordo bilaterale. Non solo, le stesse autorità garanti - cui la Corte di Giustizia ha riconosciuto un ruolo decisivo nella valutazione della legittimità dei flussi transfrontalieri verso gli USA – hanno sposato una strategia attendista.

Se si eccettua infatti la posizione del garante dello Schleswig-Holstein, le autorità nazionali, attraverso l'Article 29 Data Protection Working Party, hanno ribadito l'illegittimità dei trattamenti effettuati sulla base dell'accordo dichiarato invalido, ma nello stesso tempo hanno concesso più di tre mesi alle parti in gioco (imprese e governi) per addivenire ad una soluzione. Pronta in tal senso la reazione della Commissione Europea che ha spinto per una rapida rinegoziazione del «Safe Harbour».

[17] Cfr. a riguardo Europe-v-facebook, *Irish High Court: DPC to investigate Facebook's PRISM participation*, 21 ottobre 2010, http://www.europe-v-facebook.org/MU_HC.pdf.

Fino a qui dunque, per alcuni aspetti, un copione che si ripete, con lo scivolamento dal piano giuridico, rappresentato dal baluardo del giudizio di adeguatezza di cui all'art 26 della dir. 95/46/CE, verso il piano politico, basato su accordi bilaterali. La sensazione è che però, dopo la decisione della Corte di Giustizia ed in ragione delle motivazioni addotte dai giudici, non sia possibile una replica di quanto accaduto in passato.[18]

La conclusione in tempi rapidi di un nuovo accordo è tuttavia fortemente voluta dagli USA e dalla Commissione Europea, nonché dalle imprese interessate ai flussi transfrontalieri, laddove gli attori politici guardano al buon andamento dei rapporti bilaterali, mentre gli operatori commerciali alla semplificazione degli adempimenti in materia di tutela dei dati. Al raggiungimento di questo obiettivo pare però frapporsi il *decisum* della Corte, che ha fortemente limitato i margini di manovra (e di deroga) della Commissione.

In primo luogo va ricordato che, come correttamente evidenziato dalla Corte di Giustizia,[19] un accordo internazionale può fornire uno standard adeguato di tutela a condizione che non contenga deroghe in favore di disposizioni nazionali la cui adeguatezza in termini di tutela non è accertata o non sussiste. Nello specifico dunque, o si addiviene ad un nuovo accordo ove si prevede che le imprese aderenti non siano vincolate dalle disposizioni nazionali USA in conflitto con gli obblighi in materia di protezione dei dati personali previsti da tale accordo, oppure la riproposizione di deroghe in favore delle norme in materia di sorveglianza governativa esistenti negli USA implica necessariamente una valutazione dell'adeguatezza di quest'ultime. Valutazione che, in ragione dell'ampio spettro di intervento di tali disposizioni,[20] difficilmente pare ipotizzarsi come positiva.

Alla luce di tali punti fermi posti dalla decisione sul caso Schrems non sembra dunque più possibile per la Commissione addivenire ad un accordo sui flussi transfrontalieri verso gli USA senza che vengano meno i limiti esistenti con riguardo alla tutela offerta dall'ordinamento statunitense.

[18] Sulla valenza politica delle decisioni assunte dalla stessa Corte di Giustizia, si veda G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a* Schrems, in questoVolume.

[19] Cfr. supra nota 6

[20] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 93. Sulla natura ancora estesa della sorveglianza realizzata negli USA ad opera delle agenzie governative, anche dopo le riforme del 2013, cfr. T. Edgar, *Focusing PRISM: An Answer to European Privacy Concerns?*, in *Lawfare*, 2 novembre 2015, https://www.lawfareblog.com/focusing-prism-answer-european-privacy-concerns.

In tal senso, le autorità americane paiono aver colto il problema, come dimostrato dall'accelerazione avutasi nell'*iter* del Judicial Redress Act, che dovrebbe garantire la tutela giurisdizionale in favore dei soggetti europei interessati dal trattamento, in linea con quanto richiesto dalla Corte di Giustizia.[21] Rimane però il nodo dell'esteso ambito di operatività riconosciuto dalle leggi statunitensi alle agenzie investigative nell'accesso ai dati. Tali poteri, come rilevato dalla Corte di Giustizia, non sono compatibili con un generalizzato riconoscimento di un sufficiente livello di adeguatezza della tutela offerta dall'ordinamento statunitense.

Un accordo onnicomprensivo come il «Safe Harbour», con la previsione di ampie deroghe in favore della legislazione nazionale ed a discapito della tutela prevista per i dati personali,[22] può dunque solamente essere sostituito con un diverso accordo che ammetta solo eccezionalmente ipotesi di deroga rispetto al livello di protezione accordato.[23] Questo però richiederebbe la contemporanea riforma delle vigenti norme statunitensi che riconoscono poteri ispettivi alle agenzie governative nordamericane.[24] Per tale motivo una reale rinegoziazione dell'accordo UE-USA pare costituire più che altro una strategia di medio-lungo periodo.[25]

Quanto sopra non toglie tuttavia che le ragioni della politica possano

[21] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 95. Cfr. *infra* § 1.2.
[22] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 84.
[23] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 92 («above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary»). Cfr. in tal senso Corte di Giustizia dell'Unione europea, 8 aprile 2014, *Digital Rights Ireland* e altri, cause riunite C-293/12 e C-594/12, punto 52, http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=404932; Corte di Giustizia dell'Unione europea, 7 novembre 2013, *Institut professionnel des agents immobiliers (IPI) contro Geoffrey Englebert e altri*, C-473/12, punto 39, http://curia.europa.eu/juris/liste.jsf?num=C-473/12; Corte di Giustizia dell'Unione europea, 16 dicembre 2008, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, C-73/07, punto 56, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-73/07; Corte di Giustizia dell'Unione europea, 9 novembre 2010, *Volker und Markus Schecke e Eifert contro Land Hessen*, C-92/09 e C-93/09, punti 77 e 86, http://curia.europa.eu/juris/document/document.jsf?text=&docid=79001&pageIndex=0&doclang=it&mode=lst&dir=&occ=first&part=1&cid=406004.
[24] Cfr. Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, cit. («the US can currently show no effective means to ensure protection essentially equivalent to the level of protection guaranteed within the European Union»).
[25] Cfr. *infra* § 1.2.

indurre ad un nuovo accordo bilaterale, anche in difformità delle indicazioni della Corte di Giustizia. Certamente la validità dello stesso potrebbe essere contestata di fronte alle autorità garanti nazionali e poi posta all'attenzione della Corte di Giustizia che necessariamente dovrebbe giungere alla declaratoria di invalidità. Nell'ottica di una strategia dilatoria, questo porterebbe tuttavia a guadagnare un paio di anni e, considerata anche la congiuntura politica statunitense (elezioni presidenziali) e le trattative in corso sul fronte della Transatlantic Trade and Investment Partnership, questo potrebbe essere un tempo utile per conseguire una riforma dell'esistente quadro normativo statunitense in materia di *data protection* e di poteri delle forze di intelligence.

Nelle more di un eventuale nuovo accordo, potrebbe dunque prevalere una logica attendista, specie fra le piccole e medie imprese, in considerazione dei costi dell'eventuale adozione degli strumenti volti a legittimare i flussi transfrontalieri di dati.[26]

1.1 (segue). Strategia di medio periodo

Sebbene prevalga un certo immobilismo, in attesa di vedere cosa accadrà allo scadere dell'*ultimatum* posto dalle autorità garanti,[27] molti operatori economici si stanno interrogando su quali siano le soluzioni più idonee per offrire un'adeguata base giuridica ai flussi transfrontalieri di dati cui danno vita nel corso dello svolgimento delle proprie attività.[28] Questo anche alla luce del fatto che, come precisato dalla Corte di Giustizia, un nuovo «Safe Harbour» non sarà comunque immune dal sindacato delle autorità garanti.[29]

[26] Cfr. paragrafo successivo.

[27] Cfr. Article 29 Data Protection Working Party, *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case* (C-362-14), Brussels, 16 ottobre 2015, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf, in cui i garanti europei hanno chiarito che «If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions».

[28] Ad oggi infatti solo le imprese più lungimiranti, che avevano affiancato l'adozione delle *standard contractual clauses* ai benefici del «Safe Harbour», risultano essere in una posizione di vantaggio competitivo potendo ostentare la conformità alla legge dei propri servizi.

[29] Cfr. anche Corte di Giustizia dell'Unione europea, 1 ottobre 2015, C-230/14,

Standard contractual clauses, *binding corporate rule*s, clausole contrattuali *ad hoc*, consenso dell'interessato, sono dunque stati prontamente riscoperti dai consulenti legali ed esperti di *privacy* in tutto il mondo. Soluzioni prima accantonate perché onerose e limitanti, a fronte della maggior semplicità dell'adesione ai «Safe Harbour» Principles, sono ora prese nuovamente in considerazione dalle imprese statunitensi e dai loro *partners* europei.

Rispetto alle diverse alternative, che possono offrire non solo una pronta risposta nell'intermezzo fra il vecchio ed il nuovo «Safe Harbour», ma anche una maggior garanzia di tutela stabile per il futuro, occorre però fare dei distinguo in termini di onerosità ed efficacia.

L'opzione più semplice appare certamente quella di avvalersi del disposto dell'art 26 (a), dir. 95/46/CE, laddove si prevede che il consenso dell'interessato possa validamente legittimare il flusso di dati verso un Paese terzo. La norma, in linea con l'art. 7(a) della direttiva, richiede però che il consenso dell'interessato sia prestato «unambiguously». Posto che, ai sensi dell'art. 2(h) il consenso dell'interessato consiste nella «freely given specific and informed indication of his wishes»,[30] ne consegue che il soggetto dovrebbe ricevere adeguate informazioni circa le modalità e finalità del trattamento connesso ai flussi transfrontalieri, nonché circa gli eventuali ulteriori trattamenti posti in essere da terze parti successivamente al trasferimento dei dati. Non solo, poiché l'art. 26(a) prevede la possibilità di invio di informazioni personali verso un Paese terzo che non offre un adeguato livello di protezione in virtù del consenso dato «unambiguously», ne consegue che l'interessato dovrà quanto meno essere informato circa tale carenza di protezione ed in cosa questo si concretizzi, in termini di rischio per i dati che lo riguardano.

Questo contesto normativo esclude in primo luogo la possibilità del ricorso esteso al consenso dell'interessato al fine di legittimare una molteplicità pressoché indistinta di trattamenti.[31] Ma soprattutto, relativamente all'invio dei dati verso gli USA, implica che l'interessato dovrebbe essere consapevole dei poteri propri delle agenzie investigative statunitensi, delle

Weltimmo s. r. o. contro Nemzeti Adatvédelmi és Információszabadság Hatóság, http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=406747.

[30] Cfr. riguardo D. Beyleveld-R. Brownsword, *Consent in the law*, Oxford-Portland, 2007, 126.

[31] Cfr. Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13luglio 2011, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

conseguenze in termini di trattamento dati e delle lacune che affliggono l'ordinamento statunitense con riguardo ad un'effettiva tutela dei dati personali.[32]

A ciò si aggiunga che l'idea del consenso dell'interessato come espressione di una volontà consapevole ed informata è sempre più oggetto di critiche da parte della dottrina giuridica, stante la complessità dei trattamenti dati realizzati e la difficoltà di fornire un'adeguata e comprensibile informativa all'interessato.[33] Posto che ad oggi risultano ancora in parte oscure le articolate modalità di trattamento realizzate negli USA attraverso l'interazione fra attori pubblici e privati,[34] pare dunque viepiù improbabile che queste possano essere oggetto di un'adeguata informativa, che è il presupposto per un consenso consapevole.

Come poi correttamente sottolineato dal garante dello Schleswig-

[32] Cfr. anche Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, cit.

[33] Cfr. L. Brandimarte, A. Acquisti e G. Loewenstein, *Misplaced Confidences: Privacy and the Control Paradox*, 2010, Ninth Annual Workshop on the Economics of Information Security, http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf; J. Turow, C. J. Hoofnagle, D. K. Mulligan e N. Good, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, in *ISJLP*, 2007, 3, 723 ss., http://scholarship.law.berkeley.edu/facpubs/935; Federal Trade Commission, *Data brokers. A Call for Transparency and Accountability*, 2014, 42, http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf; R. M. Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, in *Notre Dame L. Rev.*, 2013, 87(3), 1027 ss.; D. J. Solove, *Introduction: Privacy Self-management and The Consent Dilemma*, in *Harv. L. Rev.*, 2013, 126, 1883 ss.

[34] Cfr. European Parliament, *Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy*, Strasburgo, 4 luglio 2013, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN; European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, *The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens*, 2013, 14 ss., http://info.publicintelligence.net/EU-NSA-Surveillance.pdf; European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs, *National Programmes for Mass Surveillance of Personal data in EU Member States and Their Compatibility with EU Law*, 2013, 12 ss., http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf.

Holstein,[35] l'ampiezza delle deroghe previste dall'ordinamento statunitense in favore dei servizi governativi è tale da minare significativamente i diritti fondamentali dell'individuo,[36] ragion per cui l'eventuale consenso dell'interessato si tradurrebbe nella rinuncia a far valere diritti per loro natura irrinunciabili. Va infatti rilevato come, pur riconoscendo margini di libertà all'individuo in termini di disponibilità dell'esercizio dei propri diritti della personalità,[37] permangano i limiti posti dall'irrinunciabilità del diritto stesso, che non ne consentono una compressione eccessiva basata sul consenso dell'interessato.[38]

Se si pensa dunque alla raccolta massiva e continua di informazioni realizzata dalle agenzie governative statunitensi,[39] alle capacità di impiego di software di *big data analytics* per estrarre ulteriori inferenze da tali dati ed alla mancanza di adeguate tutele per l'interessato, si evince chiaramente come il consenso ad un trattamento che implica tali conseguenze si traduca nella sostanziale parziale rinuncia alle prerogative costitutive del diritto fondamentale alla protezione dei dati riconosciuto al singolo, la cui ammissibilità contrasta con il nucleo indisponibile di tale diritto.[40]

Si deve in tal senso riflettere sul ruolo stesso riconosciuto in generale dalla direttiva comunitaria al consenso dell'interessato, che costituisce un

[35] Cfr. anche Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015*, C-362/14, cit.

[36] Cfr. artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea.

[37] Cfr. anche G. Resta, *I diritti della personalità*, in G. Alpa e G. Resta, *Le persone fisiche e i diritti della personalità, in Trattato di Diritto Civile*, diretto da R. Sacco, Torino, 2006, 560 ss.; G. Resta, *Contratto e persona*, in V. Roppo (a cura di), *Trattato del Contratto*, vol. VI, *Interferenze*, Milano, 2006, 67 ss.; A. Orestano, *La circolazione dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, vol. II, 142 ss.; V. Zeno-Zencovich, *Profili negoziali degli attributi della personalità*, in *Dir. Inf.* 1993, 545 ss. Per maggiori riferimenti dottrinali, in ragione dell'economia del presente scritto, si rinvia a A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007, 69 ss. Cfr. anche P. M. Schwartz, *Property, Privacy, and Personal Data*, in *Harv. L. Rev.*, 2003, 117, 2056 ss.; P. Samuelson, *Privacy as Intellectual Property*, in *Stan. L. Rev.*, 1999, 52, 1125 ss.

[38] Cfr. G. Resta, Il diritto alla protezione dei dati personali, in F. Cardarelli, S. Sica e V. Zeno-Zencovich (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, 53 ss.

[39] Cfr. *supra* nota 34

[40] Cfr. art. 52, c. 1, Carta dei diritti fondamentali dell'Unione europea. Cfr. anche V. Zeno-Zencovich, *Profili negoziali degli attributi della personalità*, cit., 549; C. Scognamiglio, *Il diritto all'utilizzazione economica del nome e dell'immagine delle persone celebri*, in *Dir. Inf.* 1988, 139 s.; C. Pedrazzi, voce *Consenso dell'avente diritto*, in *Enc. Dir.*, vol. IX, Milano, 1961, § 9.

presupposto di legittimazione del trattamento, ma non prescinde dalla necessaria sussistenza degli altri requisiti di liceità di quest'ultimo, *in primis* quello di proporzionalità.

Posto che anche la generazione di un flusso transfrontaliero rappresenta una modalità di trattamento, v'è da chiedersi come possa il consenso dell'interessato legittimare un flusso di dati che, per le ulteriori modalità di trattamento successive all'invio dei dati verso Paesi terzi, si configura come contrastante con i princìpi di liceità del trattamento. In proposito, pare doversi escludere che il consenso possa da solo sopperire ai limiti che connotano il trattamento in termini di proporzionalità dello stesso, ovvero alla carenza di determinatezza delle finalità o alla mancanza di trasparenza circa le modalità di gestione dei dati, tutti aspetti che ad oggi affliggono il possibile utilizzo delle informazioni ad opera delle agenzie governative statunitensi.

Va infine osservato come il ricorso al consenso dell'interessato ponga problemi specifici connessi alla diversità di disciplina esistente nei vari Paesi dell'UE con riguardo alla prestazione dello stesso (si pensi ad es. al consenso relativo ai minori per i dati che li riguardano), cui si aggiunge la difficoltà di fare ricorso a tale strumento in situazioni ove la libertà del consenso rispetto al trattamento transfrontaliero dei dati può risultare limitata o dubbia (e.g. rapporti di lavoro).

Stanti gli evidenti limiti posti ad una legittimazione dei flussi transfrontalieri incentrata sul solo consenso dell'interessato, le imprese dovranno necessariamente valutare soluzioni alternative o complementari. A tal proposito, gli strumenti che assumono maggior rilievo sono in primo luogo le già richiamate *standard contractual clauses* approvate dalla Commissione Europea,[41] cui si affiancano le c.d. Binding Corporate Rules[42] e, da ultimo,

[41] Cfr. European Commission, *Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271)*, 2004/915/EC, Annex (in seguito abbreviata come European Commission, 2004/915/EC) e European Commission, *Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593)*, 2010/87/EU (in seguito European Commission, 2010/87/EU). Cfr. anche European Commission, *Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (notified under document number C(2001) 1539)*, 2001/497/EC (in seguito European Commission, 2001/497/EC). Tutti i testi sono consultabili al seguente indirizzo: http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

[42] Cfr. Article 29 Data Protection Working Party, Working Document: Transfers

gli accordi individuali fra *data importer* e *data exporter*.

Senza qui anticipare la più dettagliata disamina di tali istituti che verrà svolta altrove,[43] va rilevato come, dal punto di vista dell'impresa, le soluzioni ora elencate comportino nuovi oneri organizzativi, che possono trovare giustificazione solo in un'ottica di medio o lungo periodo. A differenza del consenso dell'interessato, la scelta su quale fra le strategie in questione porre in essere richiede quindi una valutazione preliminare circa la natura, la complessità e la rilevanza dei flussi transfrontalieri che interessano l'impresa, nonché della continuità degli stessi nel tempo.

In tale ottica, prima ancora di optare per un rimedio o per l'altro, andrebbe accuratamente monitorato il trattamento dati in questione, valutando soluzioni di minimizzazione dell'impiego dei dati personali e, ove possibile, optando per il ricorso all'anonimizzazione. È infatti noto come le prassi operative aziendali[44] non di rado diano vita a trattamenti ridondanti, eccessivi o superflui, che già di per sé sarebbero dunque in contrasto con i princìpi del D.Lgs. 196/2003.

All'esito di tale revisione possono dunque isolarsi processi che non necessitano di essere condotti facendo uso di dati in forma nominativa. Poiché tuttavia, ai sensi dell'art. 4, c. 1, lett. b), D.Lgs. 196/2003, costituiscono dato personale anche le informazioni riferite a soggetti meramente identificabili e poiché l'identificazione può avvenire anche indirettamente «mediante riferimento a qualsiasi altra informazione», va tenuto conto che un anonimato pressoché assoluto è difficile da conseguirsi nel contesto delle moderne tecnologie di *big data analytics*.[45]

---

of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, 3 giugno 2003, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp74_en.pdf; Article 29 Data Protection Working Party, Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From «Binding Corporate Rules», 14 aprile 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_en.pdf; Article 29 Data Protection Working Party, Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 14 aprile 2005, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp108_en.pdf. Per un elenco completo dei documenti adottati dall' Article 29 Data Protection Working Party si rinvia al seguente indirizzo: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/tools/index_en.htm.

[43] Cfr. G.M. Riccio, *Gli strumenti alternativi per il trasferimento dei dati personali extra UE (clausole contrattuali standard e binding corporate rules)*, in questo Volume.

[44] Cfr. A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, cit., 87 ss.

[45] Cfr. A. Narayanan, J. Huey, E. W. Felten, *A Precautionary Approach to Big Data*

Fermo tale limite, in applicazione del principio di proporzionalità, si può comunque ritenere che ove il processo di re-identificazione richieda risorse sproporzionate e l'aggiramento di divieti di re-identificazione[46] o barriere tecnologiche, il livello di anonimato possa considerarsi sufficiente al fine di escludere i dati in questione dall'ambito di applicazione del D.Lgs. 196/2003. In relazione ai flussi transfrontalieri, dovrebbe tuttavia in questi casi prevedersi uno specifico impegno contrattuale del *data importer* a non procedere all'eventuale re-identificazione dei dati, con conseguente assunzione di responsabilità per sé per gli eventuali *sub-processors*.

Ove invece si sia necessariamente in presenza di dati personali, occorrerà ragionare in termini di adozione delle *standard contractual clauses*. Tali clausole[47] consentono di fornire un livello di tutela - ritenuto ad oggi[48]

Privacy, 2015, http://randomwalker.info/publications/precautionary.pdf; A. Narayanan, E. W. Felten, *No silver bullet: De-identification still doesn't work*, 2014, http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf; P. Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in *UCLA L. Rev.*, 2010, 57, 1701 ss.; P. Golle, *Revisiting the uniqueness of simple demographics in the US population*, in A. Juels (a cura di), *Proceedings of the 5th ACM workshop on Privacy in electronic society (ACM 2006)*, New York, NY, 2006, 77 ss.; United States General Accounting Office, *Record Linkage and Privacy. Issues in creating New Federal Research and Statistical Information*, 2011, 68 ss., http://www.gao.gov/assets/210/201699.pdf; L. Sweeney, *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, 2000, http://dataprivacylab.org/projects/identifiability/paper1.pdf; L. Sweeney, *Foundations of Privacy Protection from a Computer Science Perspective*, in *Proc. Joint Statistical Meeting, AAAS, Indianapolis (2000)*, http://dataprivacylab.org/projects/disclosurecontrol/paper1.pdf.

[46] Cfr. A. Cavoukian, D. Reed, *Big Privacy: Bridging Big Data and the Personal Data Ecosystem through Privacy by Design*, in A. Cavoukian, *Privacy by design. From rhetoric to reality*, 2014, 82 http://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf; Y. Lagos, J. Polonetsky, *Public vs. Nonpublic Data: The Benefits of Administrative Controls*, in *Stan. L. Rev. Online*, 2013 (66), 103 ss.; F. H. Cate, V. Mayer-Schönberger, *Data Use and Impact. Global Workshop*, 2013, 13, http://cacr.iu.edu/sites/cacr.iu.edu/files/Use_Workshop_Report.pdf; Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Business and Policymakers*, 2012, 21, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[47] Su cui si rinvia a G.M. Riccio, *Gli strumenti alternativi per il trasferimento dei dati personali extra UE (clausole contrattuali standard e binding corporate rules)*, cit.

[48] A seguito dei rilievi mossi dalla Corte di Giustizia non pare improbabile un'eventuale contestazione della validità delle clausole approvate dalle Commissione, ad opera delle autorità garanti nazionali. Contestazione che aprirebbe ad una sospensione dell'operatività delle stesse e, in ultima istanza, ad un'eventuale pronuncia della Corte di Giustizia sulle decisioni adottate dalla Commissione.

adeguato dalla Commissione - mediante accordi pattizi fra *data importer* e *data exporter*. Va però ricordato che, sebbene non richiesto dalla normativa italiana,[49] in diversi stati dell'Unione l'adozione di tali clausole è subordinata alla specifica approvazione dell'autorità garante locale. Questo comporta che una multinazionale potrebbe trovarsi a dover richiedere specifiche autorizzazioni per i flussi transfrontalieri generati da controllate con sede in altri Paesi dell'Unione, salva l'ipotesi di non far confluire tutti i dati in uno stato come l'Italia, ove non è richiesta un'autorizzazione specifica all'uso delle *standard contractual clauses*, e da lì generare un unico flusso verso i Paesi terzi.

Come si vede da questi pochi cenni, anche l'adozione di clausole standard implica comunque una riorganizzazione dei flussi di dati interni alle aziende o, quantomeno, nuovi specifici adempimenti. Adempimenti che non riguardano solo l'eventuale autorizzazione dell'autorità garante, ma anche quanto richiesto dalle *standard contractual clauses* in termini di *audit* e di responsabilità solidale fra *data importer* e *data exporter*.

Due sono però i principali limiti strutturali che si frappongono ad un ampio ricorso alla soluzione in esame. In primo luogo va rilevato come non vi siano clausole *ad hoc* per il trasferimento dati fra un *data processor* stabilito nell'UE ed un *sub-processor* di un Paese terzo, con la conseguenza che occorrerà ricorrere ad una delle seguenti opzioni:[50] l'impiego delle clausole-tipo comunitarie direttamente ad opera del titolare del trattamento (*controller*) mediante un accordo con il *sub-processor*; un mandato da parte del *controller* al *processor* affinché quest'ultimo stipuli in suo nome le clausole-tipo con il *sub-processor*; il ricorso a specifici accordi contrattuali fra le parti, previa autorizzazione dei competenti organi del Paese dell'esportatore.[51] Sebbene questo limite paia dunque superabile, risulta

[49] Cfr. Garante per la protezione dei dati personali, Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati in conformità alle clausole contrattuali tipo, di cui all'allegato alla decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE, 27 maggio 2010, doc. web n. 1728496, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1728496.

[50] Per un maggior dettaglio, cfr. Article 29 Data Protection Working Party, FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC, Bruxelles, 12 luglio 2010, 4 ss., in http://ec.europa.eu/justice_-home/fsj/privacy/docs/wpdocs/2010/wp176_en.pdf.

[51] Si rinvia a riguardo alle considerazioni espresse in merito al trattamento dati nel contesto dei servizi di *cloud computing*, ove è più frequente la presenza di un'ampia filiera di

comunque evidente come esso renda l'adozione delle *standard contractual clauses* onerosa.

Il secondo limite, più strettamente correlato al *decisum* della Corte di Giustizia, riguarda le previsioni contenute nella clausola II(c) delle Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers),[52] ai sensi della quale «[The data importer warrants and undertakes that:] It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws».[53] Ne consegue che, sulla base dei rilievi della Corte e delle considerazioni espresse dalla Commissione circa il livello di tutela offerto dalle normative statunitensi,[54] si dovrebbe concludere che la semplice adozione delle *standard contractual clauses* non esima dalla valutazione circa i limiti dell'ordinamento USA, ma anzi implichi la comunicazione di cui alla menzionata clausola. A seguito di tale comunicazione il *data exporter* europeo dovrebbe bloccare il flusso transfrontaliero di dati o quantomeno integrare le clausole con ulteriori e specifiche tutele, in assenza delle quali le clausole in questione potrebbero in concreto non offrire un livello adeguato di protezione.[55]

Va tuttavia rilevato come non paia emergere, a livello generale, l'intenzione delle autorità garanti europee di mettere in dubbio la validità dei

processors e *sub-processors*, in A. Mantelero, Processi di *outsourcing* informatico e *cloud computing*: la gestione dei dati personali ed aziendali, in *Dir. Inf.* 2010, 687 ss.

[52] Cfr. European Commission, 2004/915/EC, Annex, cit. Cfr. anche la clausola 5(a) delle standard contractual clauses di cui all'allegato della decisione European Commission, 2001/497/EC, cit.

[53] Cfr. anche disposizione di analogo tenore contenuta nella clausola 5(b) delle standard contractual clauses di cui all'allegato della decisione European Commission, 2010/87/EU («[The data importer agrees and warrants:] that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract»).

[54] Cfr. *supra* nota 7. [prese di posizione critiche da parte delle istituzioni comunitarie]

[55] Cfr. anche Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein, *Position Paper on the Judgment of the Court of Justice of the European Union of 6 October 2015, C-362/14*, cit.

trasferimenti effettuati avvalendosi delle *standard contractual clauses,*[56] né tantomeno la Commissione pare orientata in tal senso.[57] Come però riconosciuto dalla Commissione medesima, questo non impedisce a singole autorità garanti di valutare se tali clausole, come anche le *binding corporate rules*, possano considerarsi idonee a fornire un'adeguata protezione con riferimento a casi specifici ed a specifici Paesi terzi.[58]

Se dunque nel breve periodo l'adozione delle *standard contractual clauses* potrebbe costituire una soluzione, in un più ampio arco di tempo l'eventuale contestazione della validità delle stesseo la loro modifica ad opera della Commissione, in conseguenza della decisione che si commenta, potrebbero comportare un esito negativo per le imprese che hanno assunto i maggiori oneri derivanti dall'adozione di tali clausole.

Le medesime considerazioni paiono valide per le *binding corporate rules*, rispetto alle quali occorre poi ricordare come si tratti di una soluzione non adatta a tutte le imprese, in ragione dei costi organizzativi e del tempo necessario per la loro adozione. Se si aggiunge poi che l'approvazione delle *binding corporate rules* ad opera dell'autorità garante preposta richiede

[56] Cfr. Article 29 Data Protection Working Party, *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*, cit.

[57] Cfr. European Commission, *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, COM(2015) 566 final, Brussels, 6 novembre 2015, 5 s., http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

[58] Cfr. European Commission, *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, cit. («in the absence of a Commission finding of adequacy, the responsibility is on controllers to ensure that their data transfers take place with sufficient safeguards in accordance with Article 26(2) of the Directive. This assessment needs to be carried out in the light of all the circumstances surrounding the transfer at issue. In particular, both the SCCs and BCRs provide that if the data importer has reasons to believe that the legislation applicable in the recipient country may prevent it from fulfilling its obligations, it shall promptly inform the data exporter in the EU. In such a situation, it is up to the exporter to consider taking the appropriate measures necessary to ensure the protection of personal data. These may range from technical, organisational, business-model related or legal or measures to the possibility to suspend the data transfer or to terminate the contract. Taking into account all the circumstances of the transfer, data exporters may thus have to put in place additional safeguards to complement those afforded under the applicable legal basis for transfer to meet the requirements of Article 26(2) of the Directive»).

mediamente fra i 12 ed i 18 mesi e si guarda alla prossima applicazione del nuovo regolamento comunitario, anche qui occorre concludere che l'opzione in questione è più consona ad una strategia di lungo periodo.

Soprattutto nel caso di grandi imprese si potrà dunque vagliare quest'ultimo rimedio, che ha il beneficio di legittimare i trattamenti posti all'interno dell'organizzazione, ma si dovrà anche qui tener in conto che trattasi di una soluzione che implica la mappatura e, in molti casi, la riorganizzazione dei flussi di dati intra-gruppo, nonché la definizione di sistemi di monitoraggio successivi all'adozione delle *binding corporate rules*, la definizione di nuovi e specifici ruoli in materia di *data protection* e l'applicazione di un approccio di *privacy by design* ai processi. Un percorso dunque piuttosto oneroso, che può essere intrapreso solo se gode dell'adeguato sostegno dei vertici aziendali.

1.2 (segue). Strategia di lungo periodo e valore competitivo della tutela dei dati personali

Se nel breve periodo permane incertezza e nel medio termine si può ipotizzare l'adozione di soluzioni orientate alla tutela dei dati, ma non senza oneri ed eventuali maggior costi per le imprese, guardando al lungo periodo l'orizzonte pare potersi rasserenare.

In primo luogo, va rilevato come sul lungo periodo l'investimento in tutela dei dati sia destinato a premiare le imprese, quindi anche maggiori oneri ed adempimenti si tradurranno plausibilmente in un vantaggio competitivo.[59]

In secondo luogo, le dinamiche che si sono viste essere alla base dei rapporto fra UE ed USA in materia di trattamento dei dati e che hanno portato all'accordo «Safe Harbour» sono ragionevolmente destinate a trovare compimento. In particolare, sul versante statunitense già da tempo si assiste ad una crescente domanda da parte dei consumatori circa l'innalzamento dei livelli di protezione riconosciuti ai dati personali[60] e, sul fronte delle imprese, v'è una richiesta di standard normativi maggiormente com-

[59] In ragione dell'economia del presente scritto si rinvia a riguardo alle considerazioni espresse in A. Mantelero, *Competitive value of data protection: the impact of data protection regulation on online behaviour, in International Data Privacy Law*, 2013, 3(4), 229 ss.

[60] Cfr. M. Madden, L. Rainie, Americans' Attitudes About Privacy, Security and Surveillance, Pew Research Cente, 20 maggio 2015, http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.

patibili con quello europeo, tali da evitare uno svantaggio competitivo per le imprese USA.[61]

In quest'ultimo senso vanno le azioni intraprese ad esempio da una grande multinazionale statunitense quale Microsoft concretizzatesi nella causa contro il governo americano a difesa dell'extraterritorialità dei dati contenuti sui propri *server* situati in Europa,[62] iniziativa che ha goduto dell'appoggio di molte imprese del settore ICT.[63] In analoga direzione pare andare il supporto delle grandi imprese statunitensi ai progetti di legislazione federale volti a riformare sia l'attuale sistema di raccolta dati ad opera delle agenzie governative, sia le procedure di *mutual legal assistance*.[64]

Non è dunque un caso che un primo effetto della decisione della corte di Giustizia sia consistito nella ripresa della discussione sul Judicial Redress Act,[65] una proposta bipartisan già approvata a fine ottobre dalla House of Representatives, che riconosce anche ai cittadini europei il diritto di agire

[61] Cfr. D. Kehl, K. Bankston, R. Greene, R. Morgus, *Surveillance Costs. The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, New America's Open Technology Institute, luglio 2014, https://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf.

[62] Cfr. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 14-02985, U.S. Court of Appeals for the Second Circuit (Manhattan). Si vedano a riguardo i documenti pubblicati dall'Electronic Frontier Foundation nella pagina dedicate al caso, consultabili al seguente indirizzo: https://www.eff.org/cases/re-warrant-microsoft-email-stored-dublin-ireland. Cfr. anche Center for Democracy & Technology, *Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad?*, 30 giugno 2014, https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/.

[63] Cfr. gli Amicus Brief a support di Microsoft richiamati in Center for Democracy & Technology, *Microsoft Ireland Case: Can a US Warrant Compel A US Provider to Disclose Data Stored Abroad?*, cit.

[64] Cfr. a riguardo A. K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Era*, Global Network Initiative, gennaio 2015, http://globalnetworkinitiative.org/content/data-beyond-borders-mutual-legal-assistance-internet-era. Cfr. in merito il negoziato EU-USA sul c.d. «umbrella agreement», volto a definire un quadro comune in materia di tutela dei dati personali trattati per finalità giudiziaria, v. a riguardo European Commission, Joint EU-US Statement, Brussels, 13 novembre 2015, http://europa.eu/rapid/press-release_STATEMENT-15-6087_en.htm?locale=en; European Commission, *Questions and Answers on the EU-US data protection «Umbrella agreement»*, Brussels, 8 settembre 2015, http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm.

[65] Cfr. a riguardo E. Kelly, *Congress Moves to Give Europeans Stronger Data Privacy Rights in the U.S.*, in USA TODAY, 10 novembre 2015. http://www.usatoday.com/story/news/2015/11/10/congress-moves-give-europeans-stronger-data-privacy-rights-us/75315662/.

in giudizio di fronte alle corti statunitensi qualora il governo USA abbia avuto illegittimo accesso ai dati degli interessati.[66]

Va poi ricordato che è ancora giacente il Consumer Privacy Bill of Rights,[67] che, benché non riguardi i flussi transfrontalieri, ove si traducesse in una legge federale costituirebbe un indubbio innalzamento del livello di tutela offerto dall'ordinamento statunitense, in grado di facilitare l'affermarsi di una più forte protezione delle informazioni personali in tutti gli ambiti, compreso quello inerente l'attività delle agenzie governative.[68]

Sempre guardando alle possibili iniziative governative, va poi menzionato il negoziato in corso sul Transatlantic Trade and Investment Partnership (TTIP), fin dall'inizio visto anche come un possibile tavolo di discussione per quanto concerne gli scambi di dati. In proposito, è forte nell'Unione europea l'avversione per soluzioni liberistiche in materia di dati personali e per la stessa introduzione del tema fra i capitoli dell'accordo,[69] pare quindi improbabile che si giunga all'adozione di un testo che ricalchi il modello della Trans-Pacific Partnership. Proprio in tale ottica, i rilievi mossi dalla Corte in merito ai poteri della Commissione ed a quelli dei garanti paiono costituire forti limiti ad eventuali scorciatoie negoziali in materia di dati personali perseguibili dalla Commissione.[70]

[66] Cfr. E. Kelly, *Congress Moves to Give Europeans Stronger Data Privacy Rights in the U.S.*, cit. («The legislation would give Europeans the same protections as Americans under the Privacy Act of 1974, which governs the collection, use and dissemination of personally identifiable data contained in records held by the federal government. In addition to being able to sue the U.S. government for wilfully disclosing personal data, Europeans could sue if a federal agency refuses their request to review or amend their records. The legislation also would apply to citizens of other nations designated by the Justice Department»).

[67] Cfr. The White House, *A Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 2012, 47 s., http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[68] Va poi ricordato come la moderna sorveglianza si basi su un modello di partnership pubblico-privato, per cui il rafforzamento della tutela dei dati in mano alle imprese, l'adozione di soluzioni volte alla minimizzazione, cancellazione progressiva ed anonimizzazione dei dati, costituiscono tutti rimedi che indirettamente vengono a circoscrivere l'effetto della sorveglianza attuata dai soggetti pubblici. A. Mantelero, G. Vaciago, Digital investigation, 2015,15, 104 ss.

[69] Cfr. European Parliament, *TTIP: Trade agreements must not undermine EU data protection laws, say Civil Liberties MEPs*, 31 marzo 2015, http://www.europarl.europa.eu/pdfs/news/expert/infopress/20150330IPR39308/20150330IPR39308_en.pdf.

[70] Cfr. a riguardo la posizione espressa nel 2013 dalla Commissione Europea in European Commission, *Communication from the Commission to the European Parliament and the Council. Rebuilding Trust in EU-US Data Flows*, COM(2013) 846 final, Brussels, cit. («data protection standards will not be negotiated within the Transatlantic Trade and

Al contrario, la percezione non solo del valore economico dei dati personali, ma anche del valore competitivo della tutela delle informazioni personali, nonché le esigenze di interoperabilità dei sistemi, potrebbero indurre la controparte statunitense a perseguire con maggior decisione la strada delle riforme di cui si è detto. Questo al fine di conseguire non solo un nuovo accordo bilaterale che si sostituisca al «Safe Harbour», ma anche di orientarsi verso una più matura strategia in materia commerciale con riguardo ai dati, nel contesto dei rapporti atlantici.

Guardando, infine, alle azioni che possono essere intraprese dalle singole imprese, va segnalata la scelta della società Microsoft di adottare un modello non incentrato sulla mera delocalizzazione dei *server* nell'Unione europea, già operata da molte imprese USA (ma finora inefficace nel contrastare le norme statunitensi in materia di accesso ai dati da parte delle agenzie governative),[71] bensì imperniato su una 'delocalizzazione' del controllo. L'ipotesi allo studio pare infatti riguardare l'adozione di un modello definito di «data trustee» in cui l'impresa statunitense affida il controllo dei dati ad un *trustee* europeo,[72] che quindi opererà nell'interesse della prima, ma sarà un soggetto giuridico distinto e di diritto comunitario. Sebbene manchino sufficienti dettagli per una piena valutazione del modello, quest'ultimo, pur non facendo venir meno i flussi transfrontalieri verso gli USA, crea uno schermo giuridico all'operatività delle norme statunitensi in materia di accesso ai dati da parte delle agenzie governative,[73] operatività che costituisce la maggiore delle criticità rilevate dalla Corte di Giustizia nel caso Schrems.

Investment Partnership, which will fully respect the data protection rules»).

[71] Cfr. *supra* nota 62.

[72] Cfr. Microsoft Europe, Microsoft Announces Plans to Offer Cloud Services from German Datacenters, 11 novembre 2015, http://www.prnewswire.co.uk/news-releases/microsoft-announces-plans-to-offer-cloud-services-from-german-datacenters-545594412.html («These new cloud services will be a first of their kind innovation from a global hyperscale cloud provider, in that access to customer data stored in these new datacenters will be under the control of T-Systems, a subsidiary of Deutsche Telekom, an independent German company acting as a data trustee. Microsoft will not be able to access this data without the permission of customers or the data trustee, and if permission is granted by the data trustee, will only do so under its supervision»).

[73] Quest'ultime dovranno infatti indirizzare le proprie richieste verso una società europea e dunque avvalersi delle procedure di Mutual Legal Assistance.

2. Prime conclusioni

Al termine della disamina dei diversi scenari che la decisione della Corte di Giustizia apre con riguardo al trattamento dei dati personali posto in essere dalle imprese, non pare necessario ricapitolare quanto accennato in merito all'opportunità di una diversificazione degli approcci, dovuta sia alla tipologia dei soggetti imprenditoriali coinvolti sia alla natura dei trattamenti dati realizzati,nonché all'orizzonte temporale. Merita invece guardare oltre alle mere relazioni atlantiche e chiedersi quale sia il futuro del modello europeo di *data protection*. Un modello apparentemente vincente, capace di imporsi in molti Paesi e di condizionare l'economia globale dei dati.

Si ha tuttavia la sensazione che, portando a compimento le conseguenze desumibili dai princìpi enunciati dalla Corte, il modello si riveli più debole di quanto ora appare, incapace in concreto di difendere nella sostanza i 'confini' del proprio standard di tutela in un mondo globale ed interconnesso. Ancora forte in termini di spinta propulsiva ed in grado di innalzare il livello di protezione esistente nei Paesi terzi, ma, nel contempo, assai più fragile nella sostanza.

Accordi quali il «Safe Harbour» e rimedi quali le *standard contractual clauses*, della cui concreta operatività ben poco ci si cura, finiscono per offrire spesso più una tutela formale che sostanziale. Così come, anche all'interno dei confini dell'Unione, non mancano i tanti contrasti fra la declamazione di un elevato livello di protezione e la prassi che molte volte riduce la tutela dei dati ad una mera serie di adempimenti formali, senza poi che le informazioni beneficino di una effettiva maggior protezione.

In tale scenario la nuova proposta di regolamento comunitario apporta alcune luci (in particolare va valutato positivamente il rafforzamento dell'approccio preventivo incentrato sull'analisi del rischio), ma anch'essa, da sola, non pare riuscire a scongiurare lo iato fra *law in books* e *law in action*. Per questo, forse occorre investire maggiormente nella promozione della cultura della *privacy*. In tale ottica, l'accademia, pur nel suo raggio di azione, è chiamata ad assumere un ruolo decisivo, mettendo chiaramente in luce come il diritto del XXI secolo ed i diritti di domani si muovano soprattutto su questi terreni.[74]

[74] Cfr. a riguardo S. Rodotà, *Verso una Costituzione di Internet*, estratto dall'intervento tenuto al Convegno «Verso una Costituzione per Internet?», Roma, 16 giugno 2015, dalle ore 10, presso la Sala del Mappamondo di Palazzo Montecitorio, http://camera.civi.ci/discussion/proposals/billofrights; Camera dei deputati XVII Legislatura, Commissione per i Diritti e i Doveri in Internet, *Dichiarazione dei Diritti in*

3. «Privacy Shield». Quasi un epilogo[75]

Quanto ipotizzato nelle pagine che precedono[76] ha trovato conferma negli eventi successivi, in particolare nella nuova proposta di accordo bilaterale fra Unione Europea e Stati Uniti, denominata «Privacy Shield», e nelle reazioni che ne sono scaturite.

Nello specifico, il nuovo accordo non pare risolutivo rispetto alle criticità emerse con riguardo al previgente «Safe Harbour» ed ai rilievi formulati dalla Corte di Giustizia dell'Unione Europea nel caso Schrems. Come ipotizzato, le ragioni economico-politiche, cui si è accennato nei paragrafi che precedono, hanno indotto la Commissione Europea e le controparti statunitensi ad una rapida rinegoziazione. Quest'ultima è però avvenuta senza il coinvolgimento diretto delle autorità garanti. In questo la Commissione ha esercitato le prerogative ad essa riconosciute, ma così facendo ha marginalizzato la voce critica di tali autorità; le stesse cui compete, attraverso l'Article 29 Data Protection Working Party, il parere ad uso della Commissione sul livello di tutela offerto dai Paesi terzi,[77] nonché l'eventuale accoglimento dei ricorsi degli interessati che lamentino un inadeguato livello di protezione dei propri dati trasferiti al di fuori dei confini dell'Unione.[78]

Il diverso orientamento che è parso delinearsi con riferimento alle posizioni (più favorevoli ad un accordo di compromesso) della Commissione

Internet, 28 luglio 2015, http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/TESTO_ITALIANO_DEFINITVO_2015.pdf; L. Gill, D. Redeker, U. Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*, 9 novembre 2015, Berkman Center Research Publication No. 2015-15, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2687120.

[75] Il presente paragrafo è stato aggiunto in sede di revisione delle bozze onde dar conto dei più recenti sviluppi della materia, consistenti sia nella presentazione della bozza del nuovo accordo fra Unione Europea e Stati Uniti sui flussi transfrontalieri, denominato Privacy Shield, sia nell'approvazione della General Data Protection Regulation. Con riguardo al nuovo accordo denominato «Privacy Shield» cfr. Commissione europea, comunicato stampa del 29 febbraio 2016, disponibile al seguente indirizzo: http://europa.eu/rapid/press-release_IP-16-433_it.htm (consultato in data 1 marzo 2016); in merito al nuovo regolamento sui dati personali, cfr. invece European Commission, *Joint Statement on the final adoption of the new EU rules for personal data protection*, Brussels, 14 aprile 2016, disponibile al seguente indirizzo: http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm (consultato in data 16 aprile 2016).

[76] Cfr. *supra* §2.1.

[77] Cfr. art. 30 (1) (b), dir. 96/46/CE.

[78] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit.

e quelle (più rigorose) delle autorità garanti, in seguito alla decisione della Corte di Giustizia,[79] ha dunque trovato conferma nelle settimane successive all'accordo sul «Privacy Shield», quando ai toni trionfalistici della Commissione ha risposto un diverso atteggiamento dell'Article 29 Data Protection Working Party. Quest'ultimo, pur lodando i miglioramenti conseguiti con il nuovo accordo, non ha mancato di metterne in luce le significative criticità.

Per queste ragioni, il testo attualmente concordato fra E.U. ed USA non può considerarsi come l'epilogo della vicenda in esame. Diverse e fondatamente argomentate sono infatti le osservazioni critiche espresse dai garanti europei. Nel contempo, l'approvazione del nuovo regolamento sui dati personali (General Data Protection Regulation) implica necessariamente che 'il livello adeguato di protezione' vada rivalutato alla luce dell'innalzamento dello standard di protezione offerto dal nuovo testo normativo.[80]

Critiche sono state anche espresse dalle associazioni a tutela della *privacy*,[81] posto che gli aspetti maggiormente controversi riguardanti la proporzionalità del trattamento dati realizzato dalle agenzie governative statunitensi paiono essere ancora irrisolti.[82] In questo senso, l'accordo è

[79] Cfr. anche Article 29 Data Protection Working Party, *Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)*, Brussels, 16 ottobre 2015, disponibile al seguente indirizzo: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (consultato in data 10 novembre 2015); European Commission, *Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)*, Brussels, 6 novembre 2015, disponibile al seguente indirizzo: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf (consultato in data 10 novembre 2015).

[80] Cfr. in tal senso Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. «Privacy Shield» draft adequacy decision, Brussels*, 13 aprile 2016, disponibile al seguente indirizzo: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (consultato in data 14 aprile 2016).

[81] Cfr. la lettera inviata ai presidenti dell'Article 29 Working Party e del Committee on Civil Liberties, Justice, and Home Affairs del Parlamento Europeo, firmata da 27 delle associazioni di difesa della privacy maggiormente rappresentative in Europa e negli Stati Uniti, disponibile al seguente indirizzo: https://edri.org/transatlantic-coalition-of-civil-society-groups-privacy-shield-is-not-enough-renogitation-is-needed/ (consultato in data 18 marzo 2016).

[82] Cfr. in tal senso anche Article 29 Data Protection Working Party, *Opinion*

per lo più un compromesso volto a far fronte al vuoto creatosi in seguito all'annullamento della decisione della Commissione sull'adeguatezza del programma «Safe Harbour».

Guardando ai contenuti, l'accordo può essere diviso in due parti: una prima costituita dai Privacy Principles (allegato II) ed una seconda composta dalle dichiarazioni ed impegni adottati rispettivamente dal Governo statunitense e dai dipartimenti del commercio e della giustizia USA (allegati I e da III a VII).

Nella parte relativa ai Privacy Principles, l'accordo si mostra in grado di fornire un livello di protezione di maggior dettaglio e più elevato rispetto a quanto garantito in precedenza dal «Safe Harbour». In tal senso, aspetti positivi sono ravvisabili nell'adozione di un approccio incentrato sul rischio, in un innalzamento del livello di responsabilità dei soggetti che trattano i dati, nella definizione di procedure specifiche per i reclami inerenti ai trattamenti illegittimi, che possono essere presentati sia dai cittadini europei che dalle autorità garanti dell'Unione, ed infine nell'adozione di un sistema di monitoraggio attivo e d'ufficio da parte delle autorità statunitensi. Quest'ultime saranno dunque chiamate a verificare l'effettiva osservanza di quanto previsto dal «Privacy Shield» da parte delle imprese che vi aderiscono.

Sebbene permangano ancora zone grigie, per quanto concerne ad esempio il modello opt-out per i dati non sensibili o la lunghezza delle procedure di reclamo, i principi dettati dal nuovo accordo paiono ridurre il divario esistente fra gli standard di tutela esistenti negli Stati Uniti e nell'Unione Europea. Si tratta tuttavia di un risultato provvisorio, poiché il nuovo regolamento europeo (General Data Protection Regulation) introduce diversi mutamenti ed adotta un approccio più orientato all'analisi del rischio, aspetti che probabilmente finiranno per creare nuovamente un divario sostanziale tra le garanzie previste dalla normativa comunitaria e la protezione fornita dal «Privacy Shield».[83]

Per quanto riguarda invece la seconda parte dell'accordo (allegati I e da III a VII), essa concerne principalmente l'accesso alle informazioni e l'utilizzo delle stesse da parte delle autorità statunitensi nel caso di dati

01/2016 on the EU – U.S. «Privacy Shield» draft adequacy decision, cit.

[83] Cfr. in tal senso, Article 29 Data Protection Working Party, *Opinion 01/2016 on the EU – U.S. «Privacy Shield» draft adequacy decision*, cit., 3 («The WP29 considers a review [of the «Privacy Shield» adequacy decision] must be undertaken shortly after the entry into application of the General Data Protection Regulation, in order to ensure the higher level of data protection offered by the Regulation is followed in the adequacy decision and its annexes»).

trasferiti in ottemperanza al «Privacy Shield». Qui il testo si fa necessariamente più vago, fondandosi su assicurazioni di natura politica («il governo degli Stati Uniti ha assicurato alla Commissione che qualsiasi attività di raccolta di massa per quanto riguarda le comunicazioni via Internet che la Comunità intelligence statunitense compie attraverso i segnali di intelligence operano su una piccola parte di Internet») o rinviando a future implementazioni, quali ad esempio l'istituzione dell'Ombudsperson, che dovrà farsi carico di ricevere e rispondere ai ricorsi dei singoli che lamentino una violazione dei diritti sui dati connessa alle attività dei servizi di intelligence statunitensi.

In assenza tuttavia di cambiamenti significativi con riguardo alle pratiche di sorveglianza d'Oltreoceano ed alle norme che le regolano, pare prevalere un certo scetticismo circa il reale impatto di questa parte del nuovo accordo. In tal senso sembrano essere orientati anche i garanti europei, che hanno mosso diverse e decisive critiche al nuovo testo.

In primo luogo, i garanti sottolineano la mancanza di chiarezza espositiva, dovuta sia alla divisone in più parti dell'accordo, di cui si è detto e tale da rendere difficile una lettura organica del testo, sia alla scarsa chiarezza lessicale del testo. In secondo luogo, alcuni dei principi cardini della normativa europea non risultano essere recepiti dall'accordo (e.g. data retention principle) o sono recepiti in maniera poco lineare (e.g. purpose limitation principle). Mancano poi sufficienti garanzie circa l'eventuale successivo trasferimento dei dati inviati negli USA verso ulteriori Paesi. Lo stesso esercizio dei diritti da parte dei cittadini europei nei confronti dei soggetti che trattano i dati che li riguardano negli USA appare poi troppo complesso e di difficile praticabilità per gli interessati, tanto da far dubitare della reale efficacia del rimedio stesso.

Infine, se da un lato i garanti danno atto che il nuovo accordo affronta la questione del trattamento dati posto in essere dalle agenzie governative statunitensi, rilevano però come una raccolta massiva ed indiscriminata di dati ad opera di tali soggetti non sia esclusa e come la figura di garanzia prevista dal «Privacy Shield» (l'Ombudsperson) mostri limiti intriseci dovuti alla carenza di indipendenza e mancanza di poteri e rimedi adeguati.

La critica più incisiva pare poi quella secondo cui il testo del nuovo accordo «does not include a comprehensive assessment of the domestic law and the international commitments of the U.S. in the form of an adequacy report, as has been the regular practice in the past in similar procedures and in line with Article 25 of the Directive». Sembra quindi

essere stata disattesa proprio la richiesta implicita nella decisione sul caso Schrems, in cui la Corte di Giustizia aveva lamentato la mancanza di «sufficient findings regarding the measures by which the United States ensures an adequate level of protection, within the meaning of Article 25(6) of that directive, by reason of its domestic law or its international commitments».[84]

A sei mesi dalla decisione della Corte di Giustizia il quadro giuridico inerente i flussi transfrontalieri di dati fra Unione Europea e Stati Uniti è dunque ancora tutt'altro che definito, lasciando la prassi concreta del trasferimento dati in una sorta di limbo destinato a durare sino a quando qualche autorità garante non deciderà di intervenire rispetto all'irregolarità che connota larga parte della situazione attuale, in cui enormi quantità di dati attraversano l'Atlantico prive di adeguata legittimazione giuridica.[85]

Se a questo si aggiunge l'effetto dell'approvazione del nuovo regolamento dell'Unione sulla tutela dei dati personali e la necessaria revisione del «Privacy Shield» che ne dovrebbe conseguire,[86] si deve concludere che le strategie delineate nei precedenti paragrafi paiono rimanere valide. In tale ottica le imprese con maggior colpevolezza dovrebbero valutare l'opportunità di orientarsi verso soluzioni differenti da quelle basate unicamente sugli accordi bilaterali fra Unione Europea e Stati Uniti. Certamente si tratta di alternative più gravose,[87] ma meno suscettibili di subire i contraccolpi del delicato e variabile equilibrio di interessi che caratterizza l'economia ed il controllo dei dati, sempre più al centro dei dialoghi atlantici.

In un'ottica più ampia, l'effetto della decisione sul caso *Schrems* e la ri-definizione in corso dell'accordo bilaterale sui flussi di dati fra U.E. ed USA, così come le disposizioni contenute nel nuovo regolamento comunitario, inducono a guardare oltre al caso concreto dei rapporti atlantici per domandarsi se il modello europeo in materia di tutela dei dati dei cittadini sia davvero vincente al di fuori dei confini dell'Unione, come sembra apparire a prima vista.

[84] Cfr. Corte di Giustizia dell'Unione europea, C-362/14, cit., punto 83.
[85] Si ha avuto recente notizia di un procedimento aperto dall'autorità per la protezione dei dati personali di Amburgo; cfr. D. Windelband, *«Safe Harbour» – Hamburger Aufsichtsbehörde leitet Ordnungswidrigkeitenverfahren ein, in Datenschutz Notizen*, disponibile al seguente indirizzo: https://www.datenschutz-notizen.de/safe-harbor-hamburger-aufsichtsbehoerde-leitet-ordnungswidrigkeitsverfahren-ein-5614585/ (consultato in data 29 aprile 2016).
[86] Cfr. *supra* nota 82.
[87] Cfr. *supra* § 1.1.

Rinviando ad altra sede per più ampie considerazioni a riguardo,[88] va qui osservato come i diversi strumenti disponibili, siano essi accordi *ad hoc* come il «Privacy Shield» o decisioni sull'adeguatezza della normativa dei Paesi terzi o clausole standard, mostrano un'intrinseca debolezza dovuta alla mancanza o carenza di un'effettiva attività di monitoraggio costante dei livelli di protezione concretamente assicurati da tali strumenti. Che si tratti del rispetto delle clausole standard da parte dei contraenti o della prassi applicativa delle leggi straniere ovvero del rispetto dei 'programmi' quali il «Safe Harbour» o il «Privacy Shield» da parte dei soggetti che vi aderiscono, il rischio principale pare essere il divario tra il modello come definito dalla normativa e la prassi concreta, in termini di effettiva tutela dei diritti e delle libertà fondamentali.

In quest'ottica, si ha il sentore che le disposizioni dell'Unione in materia di flussi di dati finiscano per assumere una natura che è sovente declamatoria, la cui effettiva ragion d'essere risiede in una più ampia e complessa operazione politica. Un'operazione che può essere compresa solo guardando alla dimensione multi-stakeholder inerente la *data protection* globale, che coinvolge diverse aree economiche (USA, UE, Cina, ecc) e diverse organizzazioni (COE, APEC, OCSE, Nazioni Unite). Da questo punto di vista, le barriere legali costruite intorno ai dati europei, con i loro effetti sui flussi internazionali di informazioni, sembrano essere uno strumento per rafforzare la *leadership* dell'Unione nell'intento di definire le future linee globali in materia di protezione dei dati, piuttosto che una reale garanzia di un più elevato ed efficace livello di protezione dei dati trasferiti verso Paesi terzi. È infatti sullo scacchiere globale che si gioca la vera partita inerente i dati personali, una partita che non riguarda solo il rispetto dei diritti fondamentali, ma anche e sempre più gli assetti economici e politici.

[88] Cfr. A. Mantelero, *From Safe Harbour to Privacy Shield. The 'medieval' sovereignty on personal data, in Contratto e Impr./Europa*, 2016, in corso di pubblicazione.

Abstract

The Safe Harbour agreement was the result of an economic and political compromise between the European Union and the United States in the field of data protection, where the European regulatory model has demonstrated its influence in an interdependent world. The ECJ judgement has put an end to this compromise.

Against this background, the author points out the different solutions that private companies may adopt in the short-, medium- and long-term. In this light, the article considers the chance of reaching a new international bilateral agreement in short time and the limits posed by the ECJ decision to this potential agreement.

Focusing on the medium-term scenario, the author takes into account the impact of the Schrems case on the different legal alternatives for data transfer (data subject's consent, standard contractual clauses, and binding corporate rules) and discusses the consequences of this judgement on business strategies.

In the long-term scenario, a more optimistic outlook is possible, given the increasing demand for data protection coming from U.S. companies and society at large, as demonstrated by the support provided the U.S. business community to new regulatory initiatives and by the In re Microsoft Corp. *case.*

Giorgio Giannone Codiglione

Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali

Sommario: 1. Oggetto ed effetti della sentenza *Schrems*: protezione dei dati ed efficacia transnazionale delle tutele. – 2. Una seconda lettura: mercato dei dati e libertà d'impresa. – 3. Internet e i *social network*. – 4. Nuovi mercati rilevanti e posizioni dominanti tra UE ed USA. – 5. Convergenza dei rimedi e neutralità della rete.

1. Oggetto ed effetti della sentenza Schrems: protezione dei dati ed efficacia transnazionale delle tutele

La sentenza della Grande sezione della Corte di giustizia europea resa nel caso *Schrems* c. *Facebook* focalizza la propria attenzione sulla conformità della decisione 2000/520/CE della Commissione[1] ai parametri di 'protezione adeguata' prescritti *in primis* dalla direttiva 95/46/CE (art. 25, par. 6, nonchè artt. 7 e 8 della Carta dei diritti fondamentali[2]), con particolare riguardo al principio di effettività delle tutele di cui all'art. 47 della Carta.

Come era avvenuto nelle pronunzie «Digital rights Ireland»[3] e «Google Spain»[4], i giudici del Lussemburgo intervengono sul tema della tutela dei

[1] Commissione europea, decisione del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, in GUCE, L 215 del 25 agosto 2000, pp. 7-47.

[2] Si vedano. *ex multis* V. D'Antonio, *Il trasferimento dei dati all'estero,* sub *artt. 42 – 45*, in S. Sica – P. Stanzione (dir. da*), La nuova disciplina della privacy*, Bologna, 2005, pp. 155-197; R. Miranda, *Trasferimento dei dati all'estero*, in C.M. Bianca – F.D. Busnelli, *La protezione dei dati personali*, Padova, 2007, pp. 818 e ss.; I.J. Lloyd, *Information Technology Law*, 6th ed., Oxford, 2011, pp. 182-205.

[3] CGE Grande sez., 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital rights Ireland Ltd*, in *Dir. Inf.* 4/5, 2014, pp. 851-886.

[4] CGE Grande sez., 13 maggio 2014, causa C-131/12, *Google Spain, Google Inc.* c.

dati personali affermando e rafforzando alcuni princìpi al fine di riequilibrare il rapporto tra l'interesse pubblico alla sicurezza nazionale ed il diritto e la libertà degli utenti di conoscere e disporre dei propri dati personali veicolati sulla rete.

Nei casi citati si applica un parametro interpretativo generale di progressiva gerarchizzazione del sistema dei diritti fondamentali, che favorisce la protezione della privacy sull'interesse pubblico e quello economico dei prestatori dei servizi[5]. Tale tutela può prescindere dall'azionamento di meccanismi giurisdizionali: volendo adottare una prospettiva rimediale, il diritto fondamentale diviene giustiziabile *ex se*, permettendo una *reazione* immediata alla violazione subita.

Un altro aspetto riguarda l'efficacia territoriale delle tutele: come già è avvenuto sulla scorta del caso *Google Spain*, ove alcuni giudici o autorità amministrative hanno esteso le proprie decisioni a tutti i nomi di dominio riferibili ad un dato prestatore di servizi, chiamando in causa (o ammettendo l'intervento volontario) dell'impresa-madre (di solito ubicata in paesi extra-UE)[6]. Seguendo questo trend, nel caso *Schrems* la Corte invalida la decisione della Commissione sul c.d. *safe harbor* e afferma che ogni cittadino comunitario può adire l'autorità nazionale competente per vedere applicata la normativa sui dati personali anche qualora siano stati trasferiti in un paese terzo.

2. Una seconda lettura: mercato dei dati e libertà d'impresa

Da una attenta lettura del corpo della sentenza *Schrems*, emergono alcuni elementi che non attengono strettamente al binomio privacy individuale/sicurezza globale (una costante nel *reasoning* dei giudici del Lussemburgo), conducendo verso una questione di importanza non secondaria:

AEPD, Costeja González, ivi, pp. 535 – 562.

[5] S. Rodotà, *Solidarietà*, Bari-Roma, 2014, p. 92 s.

[6] Sul punto, paradigmatica è la recente esperienza francese: v. TGI Paris, ord. 24 novembre e 19 dicembre 2014, in *Dir. Inf.* 2015 pp. 532 e 541. Ancora in maniera più esplicita si è posta la Commission nationale de l'informatique et des libérte, affermando che la deindicizzazione, «per essere effettiva, deve essere effettuata su tutte le estensioni del motore di ricerca, senza limitazione ai soli nomi di dominio europei» (cfr. CNIL, dec. nn. 2015-047 del 21 maggio 2015, spec. p. 2 ss. e 2015-170 dell'8 giugno 2015, spec. p. 2, reperibili all'URL: www.cnil.fr/.

a) la decisione invalidata affronta il tema del trasferimento transfrontaliero di dati intesi in primo luogo come beni economici[7], scambiabili liberamente tra imprese e necessari a «promuovere lo sviluppo del commercio internazionale»[8].

Negli ultimi anni, il regime di utilizzo dei dati da parte dei prestatori ha superato la mera funzione di volano delle strategie commerciali[9] (si pensi alle preferenze d'acquisto desumibili dal c.d. *profiling* e alle proposte individuali effettuabili attraverso il *behavioural advertising*): sono i dati

[7] Il tema dell'informazione intesa come 'bene' si presta a letture diverse, a volte discordanti, strettamente connesse alla multiforme natura che essa può ricoprire (sotto un profilo soggettivo ed oggettivo), anche sincronicamente, in un determinato contesto. Ciò che si vuole rilevare in questa sede è che il regime giuridico dell'informazione in rete declinata nel senso di protezione dei dati personali rappresenta una risposta alla 'dematerializzazione' degli attributi umani in ambito digitale basato su parametri qualitativi che riguardano la classificazione del singolo dato e le modalità e tempistiche di trattamento e conservazione. Per una riflessione generale sul tema si rimanda a J. Litman, *Information Privacy/Information Property*, in 52 *Stan. L. Rev*. 1283 (2000); S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, pp. 52 e ss.; K.J. Arrow, *Il benessere economico e l'allocazione delle risorse per l'attività inventiva*, trad. it. in M. Egidi - M. Turvani (a cura di), *Le ragioni delle organizzazioni economiche*, Torino, 1994, pp. 117 - 139, spec. p. 124 s.; V. Zeno-Zencovich, voce *Informazione (profili civilistici)*, in *Dig. disc. priv*., sez. civ., IX, Torino, 1993, pp. 420 e ss.; R. Pardolesi – C. Motti, *L'informazione come bene*, in G. De Nova (a cura di), *Dalle* res *alla* new properties, Milano, 1991, p. 37 ss.; G. Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, p.209 e ss.

[8] CGE Grande sez., 6 ottobre 2015, causa C-362/14, *Maximillian Schrems* c. *Data Protection Commissioner*, parr. 8, 12 e 48: «Riconoscendo al contempo, al suo considerando 56, che i trasferimenti di dati personali dagli Stati membri verso paesi terzi sono necessari allo sviluppo degli scambi internazionali, la direttiva 95/46 pone come principio, al suo articolo 25, paragrafo 1, che siffatti trasferimenti possano avere luogo soltanto se tali paesi terzi garantiscono un livello di protezione adeguato». La dottrina ha da sempre inquadrato il trasferimento dei dati come fattore essenziale per lo sviluppo del commercio elettronico: sul punto si v. ad es. R.W. Brown, *Economic and Trade Related Aspects of Transborder Data Flow*, in 6 *Nw. J. Int'l L. & Bus.* 1 (1984); V. Frosini, *La libera circolazione dei beni e dei servizi informatici nel mercato comune europeo*, in *Dir. Inf.* 1995, spec. pp. 21 e ss.

[9] V. ad. es. il considerando 18 della direttiva 2000/31/CE: «I servizi della società dell'informazione abbracciano una vasta gamma di attività economiche svolte in linea (*on line*). Tali attività possono consistere, in particolare, nella vendita in linea di merci. […] Non sempre si tratta di servizi che portano a stipulare contratti in linea ma anche di servizi non remunerati dal loro destinatario, nella misura in cui costituiscono un'attività economica, come l'offerta di informazioni o comunicazioni commerciali in linea o la fornitura di strumenti per la ricerca, l'accesso e il reperimento di dati. I servizi della società dell'informazione comprendono anche la trasmissione di informazioni mediante una rete di comunicazione, la fornitura di accesso a una rete di comunicazione o lo stoccaggio di informazioni fornite da un destinatario di servizi. […]».

stessi l'oggetto principale dell'attività imprenditoriale. Il dato – sia personale che anonimo – viene captato, veicolato, trattato e nella maggior parte conservato ed accumulato[10], rappresentando una forma di 'capitale'[11] diverso e alternativo al plusvalore ottenuto dalla vendita dei servizi o degli spazi pubblicitari[12].

b) La nozione di 'benessere individuale'[13] richiamata è anche quella del consumatore[14]: tale aspetto è confermato dalla competenza riconosciuta nella decisione 2000/520/CE alla *Federal Trade Commission* sul controllo del trattamento dei dati trasferiti negli Stati Uniti[15].

[10] Il riferimento è ai «Big data», che rappresentano la più moderna frontiera dello sfruttamento dei dati personali connessa alla quantità delle informazioni raccolte e non alle loro intrinseche qualità. Il risultato è lo stravolgimento del ruolo del rapporto di causalità, scalzato dal concetto di «correlazione». Sul punto si rimanda all'illuminante disamina svolta da V. Mayer-Schönberger – K. Cukier, *Big data*, Milano, 2013, passim.

[11] Sulla nozione di 'capitale' e 'plusvalore' in politica dell'economia si rimanda, in una sconfinata e discordante messe di opinioni, ad es. a J. Eaton, *Economia Politica*, Torino, 1971, passim. Il tema è stato esplorato con riguardo all'attuale assetto economico, sociale e tecnologico da A. Gorz, *L'immateriale. Conoscenza, valore e capitale*, ed. it., Torino, 2003, spec. pp. 24 e ss.

[12] Secondo alcune stime, il valore creato dalle nostre identità digitali in Europa corrisponderà ad oltre 1 trilione di euro entro il 2020, ossia circa l'8% del PIL combinato dei 27 paesi UE. L'uso dei dati personali porterà un beneficio economico, ovviamente non solo per aziende private, di 330 miliardi di euro l'anno entro il 2020. Così Boston Consulting Group, The Value of our Digital Identity, reperibile all'URL: https://www.bcgperspectives.com/content/articles/digital_economy_consumer_insight_value_of_our_digital_identity/.

[13] Considerando 2 della direttiva 95/46/CE, richiamato dalla sentenza *Schrems* al par. 3.

[14] CGE Grande sez., 6 ottobre 2015, causa C-362/14, cit., par. 9.

[15] Alla base di tale effetto confusorio tra le aspettative di tutela europee e i rimedi statunitensi vi è la differente percezione, consistenza e il ruolo che la privacy ha da sempre svolto nei due continenti. Si ponga solo mente al fatto che proprio uno dei padri del c.d. *right to let be alone*, Louis Brandeis, si occupò di riformare la *Federal Trade Commission* investendola di «un ampio e flessibile mandato» con poteri che ne favorisserol'adattamento al mutare dei tempi, intorno al 1912, a cavallo tra la pubblicazione del celebre saggio *The Right To Privacy* sull'*Harvard Law Journal* (1890) e la cristallizzazione per via giurisprudenziale di quei principi in *Olmstead v. United States*, 277 U.S. 438 (1928). In argomento v. M. Winerman, T*he Origins of the FTC: Concentration, Cooperation, Control, and Competition*, in *71 Antitrust L. J.* 1 (2003). Commissione europea, decisione 2000/520/CE, cit., all. II, FAQ 11: «[…] La Commissione federale per il commercio (FTC) si è impegnata ad esaminare in via prioritaria i casi trasmessi da organizzazioni di autoregolamentazione in materia di riservatezza (quali BBBOnline e TRUSTe) e dagli Stati membri dell'UE per denunciare la presunta non conformità ai principi dell'approdo sicuro, al fine di stabilire se vi siano state violazioni della sezione 5 del FTC Act, che vieta azioni o pratiche sleali od ingannevoli nel commercio […]». Si vedano anche i paragrafi 44 e 205 delle conclusioni dell'avvocato generale Yves Bot sul caso *Schrems*, presentate

c) La tutela dei dati personali è rappresentata come un fattore che condiziona il perseguimento dell'interesse economico, imponendo alle imprese dei costi 'normativi' che influenzano in via mediata l'assetto generale del mercato. Come è stato rilevato dalla Commissione in alcune comunicazioni (che anticipano gli esiti della sentenza in commento), la creazione di un 'canale preferenziale' di trasferimento di dati tra un paese comunitario ed un paese terzo sfavoriva le imprese unicamente operanti in Europa poiché, di fatto, venivano eluse le normative sulla sicurezza dei dati e la durata del trattamento per scopi di interesse generale come emerso dallo scandalo Snowden-NSA[16]) e in senso più ampio si creava un vantaggio competitivo in termini di costi di conformazione ai concorrenti con sede sul territorio statunitense[17].

il 23 settembre 2015: «La competenza della FTC è limitata agli atti e alle pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, ed essa non si estende pertanto alla raccolta e all'impiego di informazioni personali a fini non commerciali. L'ambito di competenza limitato della FTC restringe il diritto dei singoli alla protezione dei loro dati personali. La FTC è stata creata non già per assicurare la protezione del diritto individuale alla vita privata, come avviene in seno all'Unione per le autorità nazionali di controllo, bensì per garantire un commercio leale ed affidabile per i consumatori, il che limita, *de facto*, le sue capacità di intervento nella sfera relativa alla protezione dei dati personali. La FTC non svolge pertanto un ruolo equiparabile a quello delle autorità nazionali di controllo previste all'articolo 28 della direttiva 95/46».

[16] F. Bignami, *European Versus American Liberty: A Comparative Privacy Analysis Of Antiterrorism Data Mining*, in 48 *B.C. L. Rev.* 609 (2007); P.M. Schwartz, *The Eu-U.S. Privacy Collision: A Turn To Institutions And Procedures*, in 126 *Harv. L. Rev.* 1966 (2013).

[17] CGE Grande sez., 6 ottobre 2015, causa C-362/14, cit., par. 24: «Secondo il punto 8 della comunicazione COM(2013) 847 final, fra le imprese certificate figuravano «[l] e imprese del web come Google, Facebook, Microsoft, Apple, Yahoo», le quali contano «milioni di clienti in Europa» e trasferiscono dati personali negli Stati Uniti a fini del loro trattamento».Comunicazione della Commissione al Parlamento europeo e al Consiglio del 27 novembre 2013, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, COM(2013) 846 final, p. 7: «A causa di una mancanza di trasparenza e di carenze nell'attuazione, alcuni membri auto-certificati del regime non ne osservano, in pratica, i principi. Questo ha un impatto negativo sui diritti fondamentali dei cittadini dell'UE, e mette inoltre in svantaggio le imprese europee rispetto alle loro concorrenti americane che operano nell'ambito dello stesso regime ma che in pratica non ne rispettano i principi. Questi squilibri incidono anche sulla maggior parte delle imprese americane che invece applicano correttamente il regime. Approdo sicuro funge inoltre da interfaccia per il trasferimento di dati personali di cittadini dell'UE dall'Unione europea agli Stati Uniti da parte di imprese che sono tenute a consegnare dati ai servizi di intelligence americani nell'ambito dei programmi di raccolta statunitensi. Se le carenze riscontrate non vengono corrette, si crea pertanto uno svantaggio competitivo per le imprese dell'UE e un impatto negativo sul diritto fondamentale alla protezione dei dati dei cittadini dell'Unione».Comunicazione della Commissione del 27 novembre 2013, *Sul funzionamento*

Il tema del 'costo della privacy' nel senso di analisi dell'impatto della regolamentazione sull'attività di impresa, è stato ampiamente esplorato dalla dottrina[18], sulla falsariga di quanto fatto per le regole di responsabilità civile e vicaria del *provider*[19].

In questo caso, invece, a meritare una riflessione è il rapporto 'inverso' tra libertà costituzionale d'impresa (artt. 16 della Carta e art. 41 Cost.)[20] e trasferimento dei dati personali, nel complessivo assetto concorrenziale modulare e multilivello della rete[21], tenendo in debita considerazione l'opportunità di una progressiva convergenza dell'efficacia operazionale delle normative di settore[22].

del regime 'Approdo sicuro' dal punto di vista dei cittadini dell'UE e delle società ivi stabilite, COM(2013) 847 final, p. 14: «Le carenze sopra indicate in materia di trasparenza e di applicazione suscitano preoccupazione fra le imprese europee per quanto riguarda l'incidenza negativa del regime Approdo sicuro sulla loro competitività. Una società europea che compete con una società statunitense operante nell'ambito di Approdo sicuro senza applicarne i principi si trova rispetto ad essa in una situazione di svantaggio».

[18] Si vedano ad es. G.S. Grossmann, *Transborder Data Flow: Separating the Privacy Interests of Individuals and Corporations*, in *Nw. J. Int'l L. & Bus*. 1 (1982); A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007, spec. pp. 87-201.

[19] V. ad es. G.M Riccio, *La responsabilità civile degli Internet providers*, Torino, 2002; A.C. Yen, *A Preliminary Economic Analysis of Napster: Internet Technology, Copyright Liability, and the Possibility of Coasean Bargaining*, in 26 *U. Dayton L. Rev.* 248 (2001); W.M. Landes – D.G. Lichtman, *Indirect Liability for Copyright Infringement: An Economic Perspective*, *J. M. Olin Program in Law and Economics Working Paper n. 179*, 2003.

[20] Per una visione d'insieme cfr. F. Galgano, *Sub art. 41*, in F. Galgano – S. Rodotà, *Rapporti economici*, II, *Commentario della Costituzione a cura di G. Branca*, Bologna-Roma, 1982, spec. pp. 61 e ss.; G. Amato, *Il mercato nella Costituzione*, in *Quad. cost*., 1992, pp. 7 e ss.

[21] Multilivello perché si sviluppa su più piani (infrastruttura, gestione, accesso, servizi), modulare perché l'interazione tra *device*, rete e servizi si presta al reciproco dialogo ed interconnessione. Per un primo quadro d'insieme dei rapporti tra libertà d'impresa ed Internet v. V. Zeno-Zencovich, *Internet e concorrenza*, in *Dir. Inf.* 4/5, 2010, pp. 697 e ss.; Id., R. Pardolesi, *La concorrenza sleale nell'era di Internet*, in R. Pardolesi – R. Romano, *La concorrenza reale e la tutela dell'innovazione*, in *Diritto civile*, vol. IV, t. I, dir. da N. Lipari – P. Rescigno, coord. da A. Zoppini, Milano, 2009, pp. 105 e ss.; V. Zeno-Zencovich, *I rapporti tra gestori di reti e fornitori di contenuti nel contesto europeo*, in *Dir. Inf.* 2004, pp. 421 e ss.; G. Rossi, *Cyber-antitrust, Internet e tutela della concorrenza*, in *Dir. Inf.* 2003, pp. 247-279; A. Gentili, *Internet e antitrust*, in *AIDA*, 1996, pp. 45-58; G.M. Riccio, *Concorrenza sleale e tutela dei consumatori nelle reti telematiche*, in *Dir. Inf.*, 3, 2006, pp. 307 e ss.; G. Gorkaynak - D. Durlu - M. Hagan, *Antitrust on the Internet: a Comparative Assessment of Competition Law Enforcement in the Internet Realm*, in 14 *Bus. L. Int'l* 51 (2013); F. Cugia di Sant'Orsola - R. Noormohamed – D. Alves Guimarães, *Communication and Competition Law*, Alphen aan den Rijn, 2015, spec. pp. 69 e ss.

[22] Questo tema è stato recentemente oggetto di grande attenzione da parte della dottrina

La sentenza *Schrems* non modifica in maniera definitiva una prassi diffusa quale quella del trasferimento transnazionale dei dati: in attesa di un nuovo accordo, infatti, esistono ed operano modalità differenti ed alternative per garantire l'appropriabilità e la trasferibilità dei dati personali da un server all'altro, eludendo, o comunque minando il complessivo obiettivo di tutela di stampo comunitario[23].

Non viene ad esempio censurata l'efficacia dell'atto di registrazione (o di successiva cancellazione) alle piattaforme di *social networking*[24], espressione più moderna ed istantanea di 'consenso' al trattamento dei propri dati.

L'argomento appare meritevole di un approfondimento almeno sotto tre aspetti, tra di essi collegati:

1. Ove si inquadri la libertà d'impresa come precondizione necessaria alla realizzazione di un sistema economico proteso verso il progresso[25] e l'innovazione[26], si è sostenuto come sia necessario favorire l'accesso al mercato di più imprese e, al contempo, incentivare le dinamiche

statunitense e, al contempo, di enti ed autorità di stampo comunitario: si vedano ad es. Commissione europea, *Strategia per il mercato unico digitale in Europa*, 6 maggio 2015, COM(2015) 192 final; European Data Protection Supervisor, *Privacy and competitiveness in the age of big data, Bruxelles*, 5/2014; European Parliament - Directorate General For Internal Policies Policy Department A: Economic And Scientific Policy, *Challenges for competition policy in a Digitalised Economy*, IP/A/ECON/2014-12, Bruxelles, 7/2015, spec. pp. 25 e ss.; P. Jones Harbour, *The Transatlantic Perspective: Data Protection and Competition Law*, in H. Hijmans – H,Kranenborg (a cura di), *Data Protection anno 2014: How to Restore Trust?: Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, Bruxelles, 2014, p. 25 ss.; A.P. Grunes, *Another Look at Privacy*, in 20 *Geo. Mason L. Rev.* 1107 (2013); N. Newman, *Search, Antitrust, and the Economics of the Control of User Data*, in 31 *Yale J. on Reg.* 401 (2014).

[23] In argomento si rimanda ai contribuiti di G.M. Riccio, *Model contract clauses e corporate binding rules: valide alternative al Safe harbor agreement?* e A. Mantelero, *Il trattamento dati nelle imprese nel post Safe harbour. Strategie di breve, medio e lungo periodo,* in questo Volume.

[24] CGE Grande sez., 6 ottobre 2015, causa C-362/14, cit., par. 27: «Chiunque risieda nel territorio dell'Unione e desideri utilizzare Facebook è tenuto, al momento della sua iscrizione, a sottoscrivere un contratto con Facebook Ireland, una controllata di Facebook Inc., situata, da parte sua, negli Stati Uniti».

[25] T. Ascarelli, *Teoria della concorrenza e dei beni immateriali*, Milano, 1956, p. 12 ss.

[26] Ad esempio nel senso di sviluppo tecnologico ed innalzamento della qualità dei servizi resi: F.A. von Hayek, *New Studies in Philosophy, Politics, Economics and the History of Ideas*, London, 1978, pp. 148-149: «Only when a great many different ways of doing things can be tried will there exist such a variety of individual experience, knowledge and skills, that a continuous selection of the most successful will lead to steady improvement».

'naturali' della concorrenza, limitando, ove possibile, gli interventi regolatori e/o di carattere sanzionatorio/conformativo[27].

La rete però, come d'altronde è accaduto negli ultimi due secoli con la maggior parte dei mezzi di comunicazione di massa, si presta alla formazione di monopoli ed oligopoli[28].

2. L'esistenza di posizioni di vantaggio affida nelle mani di soggetti privati un 'patrimonio informazionale' che, da una parte, aumenta la forza degli stessi nei confronti dei concorrenti e, dall'altra, corrisponde ad immense porzioni di potere pubblico.

3. L'affermata natura di Internet quale bene essenziale[29] (non solo di carattere economico ai sensi dell'art. 36 della Carta[30]) e la presenza di

[27] Una delle teorie economiche maggiormente diffuse nell'ultimo sessantennio, propugnata dalla c.d. Scuola di Chicago, ha adottato l'efficienza del sistema economico come obiettivo generale del diritto della concorrenza: M. Friedman, *Capitalismo e libertà*, ed. it., Pordenone, 1987, p. 26 s.: «l'esistenza di un libero mercato naturalmente non elimina il bisogno di un governo. Al contrario, il governo è essenziale sia come foro per la fissazione delle regole del gioco, sia come arbitro per l'interpretazione delle regole stesse per imporne il rispetto. Il merito del mercato è quello di ridurre enormemente il numero delle questioni che devono essere decise per via politica, e quindi di ridurre al minimo l'area di diretto intervento del governo nel gioco». V. anche D.D. Friedman, *L'ordine del diritto*, Bologna, 2004, spec. pp. 459 – 492 e R. Cooter – U. Mattei – P.G. Monateri – R. Pardolesi – T. Ulen, *Il mercato delle regole*, I, 2ª ed., 2006, pp. 26 e ss.

[28] R. Mansell – M. Javary, *Emerging internet oligopolies: a political economy analysis*, in E.S. Miller – W.J. Samuels, *An Institutionalist Approach to Public Utilities Regulation*, East Lansing, 2002, pp. 162-201. Si pensi alle vicende sulla gestione delle reti telefoniche negli Stati Uniti e, ancora, a quelle che hanno interessato la televisione italiana sin dalla sua nascita: F. Cairncross, *La fine delle distanze*, trad. it., Milano, 2002, pp. 281 e ss.; J. Ryan, *Storia di Internet e il futuro digitale*, Torino 2011, pp. 71 e ss.; J. Rifkin, *La società a costo marginale zero*, Milano, 2014, spec. p. 286 s.; A. Gentili, *La concorrenza nelle telecomunicazioni*, in *AIDA*, 1995, pp. 21 e ss.; R. Pardolesi, *Antitrust e multimedialità*, ivi, pp. 93-103; F. Cardarelli – V. Zeno-Zencovich, *Il diritto delle telecomunicazioni. Principi, normativa, giurisprudenza*, Bari, 1997; V. Zeno-Zencovich, *Plurality of political opinions and the concentration of media,* in 16 *Cardozo El. L.* Bull 1 (2010); S. Sica – V. Zeno-Zencovich, *Manuale di diritto dell'informazione e della comunicazion*e, 3ª ed., Padova, 2015, p. 89 e ss..

[29] In giurisprudenza si rimanda, tra le decisioni più rappresentative, alle massime affermate in *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997); Conseil Constitutionnel, 10 giugno 2009, n. 580, in *Dir. Inf.* 2009, p. 524 ss., trad. e nota di G. Votano; BGH, 14 maggio 2013, III ZR 98/12, in *Dir. Inf.* 2013, pp. 541 e ss., trad. e n. di G. Giannone Codiglione

[30] L'art. 36 della Carta dei diritti fondamentali dell'Unione europea, ricompreso al capo IV, della solidarietà, riconosce e afferma l'autonomo diritto all'accesso ai servizi d'interesse economico generale «al fine di promuovere la coesione sociale e territoriale

principi immanenti alla sua genesi e natura (quale quello di neutralità della rete), contrasta con l'interesse economico sotteso alla prestazione di servizi, facendo emergere l'importanza di declinare la libertà d'impresa come diritto strumentale alla tutela ed al soddisfacimento dei diritti fondamentali dell'individuo.

Non si può pertanto guardare al limite dell'utilità sociale solo come garanzia dell'abbassamento dei 'prezzi' (si pensi al paradosso della gratuità dei servizi web) e l'innalzamento della qualità e l'accessibilità di un prodotto o servizio in Internet, ma è forse opportuno concentrare l'attenzione sugli effetti trasversali che la garanzia di una reale competizione tra operatori sortisce in un mercato solo all'apparenza modulato su parametri ordinari[31].

3. Internet e i social network

Questa breve disamina si focalizzerà sul mercato della prestazione dei servizi di *social networking*, implicitamente investito dalla pronuncia della Grande sezione ed esempio paradigmatico della repentina ascesa di determinate figure imprenditoriali in Internet.

I *social network* forniscono servizi di comunicazione e condivisione di contenuti digitali destinati a più utenti registrati e legati tra di loro da un vincolo virtuale di amicizia che sovente è precondizione dell'interazione stessa[32].

Dall'altra parte, operando in un mercato che gli economisti hanno definito *two-* (o *multi-*) *sided*[33], essi offrono sincronicamente ad altri soggetti privati servizi e spazi pubblicitari, consistenti ad esempio nell'elabo-

dell'Unione».

[31] Si rifletta ad esempio sulle dinamiche attinenti i requisiti di accesso, sulla natura e raccolta dei proventi, o ancora sulle tipologie e modalità di erogazione del servizio.

[32] Sul punto si rinvia a S. Sica – G. Giannone Codiglione, *I social network sites e il 'labirinto' delle responsabilità*, in Giur. mer., 12, 2012, pp. 2714 – 2733; S. Vigliar, *Consenso consapevolezza e responsabilità*, Padova, 2012; G.M. Riccio, *Social networks e responsabilità civile*, in Dir. Inf. 6, 2010, pp. 859 e ss.; V. D'Antonio – S. Vigliar, *Studi di diritto della comunicazione. Persone, Società e Tecnologie dell'Informazione*, Padova, 2009, pp. 87 e ss.; G. Riva, *I social network*, Bologna, 2010.

[33] Sul punto v. M. Colangelo – V. Zeno-Zencovich, *La intermediazione on-line e la disciplina della concorrenza: i servizi di viaggio, soggiorno e svago*, in *Dir. Inf.*, 2015, spec. pp. 49-56; D.S. Evans – R. Schmalensee, *The Antitrust Analysis of Multi-Sided Platform Businesses*, Coase-Sandor Institute for Law & Economics Working Paper No. 623, 2012.

razione di appositi studi desunti dalle informazioni relative alle interazioni e alle semplici azioni poste in essere sulla piattaforma, o ancora riguardanti la comunicazione di messaggi pubblicitari ai propri utenti registrati.

Sotto un profilo classificatorio, i *social network* (o SNs) si pongono a cavallo tra i *caching* e gli *hosting providers* di cui alla direttiva 2000/31/CE: la loro attività è infatti volta a favorire la trasmissione di informazioni da un destinatario all'altro del servizio (art. 13 dir. cit.) e a memorizzare informazioni fornite da un destinatario del servizio (art. 14 dir. cit.)[34].

Volendo adottare una diversa prospettiva, non necessariamente collegata alle regole di responsabilità civile degli ISP, essi sono più semplicemente degli *edge providers*, differenziandosi dalle *backbone networks*, le compagnie che approntano grandi reti in fibra in tutto il mondo e ancora dai *broadband providers*, le imprese che forniscono servizi dati di tipo domestico, professionale o individuale.

Secondo una recente ricerca pubblicata dall'Eurostat[35], il 46% della popolazione europea attiva su Internet compresa tra i 16 e i 74 anni utilizza la rete per il *social networking*, avendo accesso a piattaforme quali *Facebook* e *Twitter*.

Sotto il profilo della tipologia del servizio reso, il mercato dei *social network* si distingue per il fatto che in genere nessuno degli operatori offra agli utenti lo stesso identico servizio: ogni prestatore difficilmente trova a confrontarsi direttamente con un avversario nel proprio settore di competenza[36].

[34] In termini di responsabilità aquiliana, nella giurisprudenza dell'ultimo decennio il problema si è 'risolto' nella definizione del parametro di 'effettiva conoscenza' di un'eventuale attività illecita posta in essere sulla piattaforma, a volte modulato rispetto all''effettivo controllo' delle informazioni veicolate: per un quadro della giurisprudenza italiana cfr. Trib. Milano, 9 settembre 2011, in *Giur. it*., 2012, p. 4; Trib. Roma, 16 giugno 2011, in Dir. ind., 2012, 1, p. 79 ss.; Trib. Roma, 16 dicembre 2009, in *Dir. Inf.* 2010, p. 278 ss., n. L. Guidobaldi; Trib. Roma, 15 aprile 2010, in *Riv. dir. ind.*, 2010, II, p. 248 ss., n. D. Mula; Trib. Roma, 22 marzo 2011, in *Danno e resp.*, 7, 2011, pp. 753 – 764, n. G.M. Riccio; Trib. Firenze, 25 maggio 2012, in *Dir. Inf.* 2012, 6, 1210 (s.m.), n. T. Scannicchio, e in Corr. giur., 4, 2013, pp. 505 – 510, n. S. Sica. In dottrina v. da ultimo M. Bassini, *La rilettura giurisprudenziale della disciplina sulla responsabilità degli Internet service provider. Verso un modello di responsabilità 'complessa'?,* in *federalismi.it,* 9/2015 e L. Bugiolacchi, *Ascesa e declino della figura del provider «attivo»? Riflessioni in tema di fondamento e limiti del regime privilegiato di responsabilità dell'hosting provider*, in *Resp. civ. prev.*, 4, 2015, pp. 1261 e ss.

[35] Eurostat, *Information society statistics - households and individuals*, 6/2015, p. 5, reperibile all'URL: http://ec.europa.eu/eurostat/statistics-explained/.

[36] Questa situazione si avvicina alla c.d. concorrenza monopolistica, in cui in un mercato senza barriere in entrata, un certo numero di imprese minori si affianca ad un operatore

Volendo semplificare e fornire al contempo dei dati indicativi sul numero di utenti registrato singolarmente ad ogni *network*, si può distinguere tra:

1. SNs generalisti (offrono servizi base di comunicazione e condivisione di media e messaggi): *Facebook*, *Twitter* (che a differenza del primo impone un limite di lunghezza ai messaggi pubblici) e *Google+* (che sfrutta indirettamente la fama del *search engine* e dei servizi di mailing offerti), si collocano ai primi posti in assoluto rispetto al numero di iscritti (rispettivamente 82%, 60%, 52%) e attivi (42%, 22%, 21%)[37]; il medesimo fenomeno si registra ad esempio in Asia, dove solo poche piattaforme generaliste attraggono il maggior numero di internauti[38].
2. SNs specialisti (dedicati ad una determinata categoria di utenti o di media oggetto dell'interazione): *Linkedin* (professionisti), *Academia* (ricercatori), *Instagram* (foto amatoriali), *Flickr* (fotografia professionale), *Last.fm* (gusti musicali) e detengono quote minoritarie, ancorchè in crescita del numero complessivo di utenze registrate ed attive.

In poco meno di dieci anni, *Facebook* e *Twitter* hanno acquisito più di cinquanta imprese a testa, tra le quali spiccano *Instagram* (2011) e il colosso delle chat vocali per telefonia mobile *Whatsapp* (2014), o ancora *Periscope*, la *mobile-app* per effettuare *streaming* video in diretta (2015)[39].

L'utente, per accedere ai servizi deve registrarsi (c.d. piattaforma chiusa), accettando le condizioni generali d'utilizzo – comprensive delle clausole di comportamento e di esonero dalla responsabilità del prestatore,

---

di maggiori dimensioni (c.d. incumbent) offrendo prodotti e servizi simili, ma distinguibili per alcune particolari qualità. Guardando alla situazione dei *social network*, si potrebbe discorrere di una concorrenza non basata sul prezzo, ma sull'appetibilità del servizio offerto. Ove si ravvisassero delle barriere in entrata per le altre imprese (legali, strategiche, reputazionali, economie di scala), si discuterebbe invece di un oligopolio. Sul punto v. H. Levy, *Monopole, Kartelle und Truste in ihren Beziehungen zur Organisation der kapitalistischen Industrie: Dargestellt an der Entwicklung in Grossbritannien*, Jena, 1909; P.S. Labini, *Oligopolio e progresso tecnico*, 2ª ed., Torino, 1967, pp. 31 e ss.

[37] GlobalWebIndex, *Quarterly report on the latest trends in social networking*, 1/2015, p. 5 ss. Lo studio è svolto quadrimestralmente, in base ai dati raccolti su un campione di 200.000 utenti intervistati in 33 paesi del globo.

[38] In Cina sono Sina Weibo, Qzone e Tencent Weibo (tutti di tipo generalista) ad avere il maggior numero di utenti iscritti ed attivi.

[39] Le liste complete sono consultabili su Wikipedia, *List of mergers and acquisition by Facebook* (12/11/2015): https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Facebook/; List of mergers and acquisition by Twitter (12/11/2015): https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Twitter/.

le licenze d'uso sui contenuti immessi[40] – e prestando contestualmente il consenso al trattamento dei dati personali[41].

L'iscrizione può essere effettuata indifferentemente e discrezionalmente su ogni piattaforma: i dati immessi e prodotti all'interno del singolo *network*, proprio a causa di tali barriere contrattuali in entrata, non possono essere cancellati e sottratti in maniera univoca, né agevolmente trasferiti da un sito all'altro[42].

Tale ragionamento può essere esteso ai legami di amicizia virtuale intercorrenti tra un utente e l'altro: una volta avviata ed implementata quella cerchia di relazioni ramificate che permette di 'connetter(c)i e rima-

[40] Dai termini d'uso di Facebook (12/11/2015): «[…] l'utente ci fornisce una licenza non esclusiva, trasferibile, che può essere concessa come sottolicenza, libera da royalty e valida in tutto il mondo, che consente l'utilizzo dei Contenuti PI pubblicati su Facebook o in connessione con Facebook ('Licenza PI'). La Licenza PI termina nel momento in cui l'utente elimina il suo account o i Contenuti PI presenti nel suo account, a meno che tali contenuti non siano stati condivisi con terzi e che questi non li abbiano eliminati. Quando l'utente li elimina, i Contenuti PI vengono eliminati in modo simile a quando si svuota il cestino del computer. Tuttavia, è possibile che i contenuti rimossi vengano conservati come copie di backup per un determinato periodo di tempo (pur non essendo visibili ad altri). […]». Dai termini d'uso di Twitter (12/11/2015): «L'utente manterrà i propri diritti sui Contenuti che invierà, posterà o renderà disponibili sui Servizi, o mediante gli stessi. Con l'invio, la pubblicazione o visualizzazione di Contenuti sui Servizi, o mediante gli stessi, l'utente concede a Twitter una licenza mondiale, non esclusiva e gratuita (con diritto di sublicenza) per l'utilizzo, copia, riproduzione, elaborazione, adattamento, modifica, pubblicazione, trasmissione, visualizzazione e distribuzione di tali Contenuti con qualsiasi supporto o metodo di distribuzione (attualmente disponibile o sviluppato in seguito). […] la presente licenza autorizza Twitter a rendere i Tweet dell'utente realizzati tramite i Servizi Twitter disponibili al resto del mondo e autorizza altri soggetti a fare altrettanto. […]Twitter potrà modificare o adattare i Contenuti dell'utente al fine di trasmetterli, visualizzarli o distribuirli attraverso reti informatiche e vari supporti e/o apportare le modifiche ai Contenuti che saranno necessarie per renderli conformi e adattarli agli eventuali requisiti o restrizioni di qualsiasi rete, dispositivo, servizio o supporto. […]».

[41] R. Caterina, *Cyberspazio, social network e teoria generale del contratto*, in *AIDA*, 2011, p. 96 e ss.; S.A. Cerrato, *I rapporti contrattuali (anche associativi) tra i soggetti del social network*, ivi, pp. 189 – 191; P. Sammarco, *Le clausole contrattuali di esonero e trasferimento della responsabilità inserite nei termini d'uso dei servizi del web 2.0*, in *Dir. Inf.* 4/5, 2010, p. 631 e ss.; F. Agnino, *Disponibilità dei diritti nei s.n.: fino a che punto è possibile disporre contrattualmente dei propri diritti? (vedi contratto fb)*, in Giur. mer., 2012, p. 2556 e ss.; S. Scalzini, *I servizi di online social network tra privacy, regole di utilizzo e violazione dei diritti dei terzi*, ivi, pp. 2570 e ss.

[42] M. Granieri, *Le clausole ricorrenti nei contratti dei social networks dal punto di vista della disciplina consumeristica dell'Unione europea*, in *AIDA*, 2011, cit., p. 125 e ss.; S. Sica – G. Giannone Codiglione, *I social network sites e il 'labirinto' delle responsabilità*, cit., p. 2724.

nere in contatto con le persone della (nostra) vita'[43], all'atto della rimozione del proprio profilo (o della cancellazione senza preavviso disposta dal prestatore), non è possibile portare in dote quel bagaglio di collegamenti relazionali in maniera semplice ed intuitiva.

La dislocazione geografica della struttura societaria si connota per la presenza di una sede centrale ubicata in territorio statunitense ed alcuni stabilimenti in Europa che svolgono per lo più mansioni di gestione dei nomi di dominio nazionali ai fini della vendita e la raccolta di proventi di carattere pubblicitario.

Sotto un profilo tecnico, la maggior parte dei dati personali raccolti dai *social network* transitano quindi oltreoceano al fine di essere trattati e/o conservati dalla casa-madre: attualmente *Facebook* utilizza quattro *data-center* negli Stati Uniti e uno in Svezia; *Twitter* invece sfrutta *data-center* già esistenti corrispondendo delle quote di locazione degli spazi ai gestori, anch'essi tutti operanti all'interno del territorio statunitense[44].

Le attività svolte dai responsabili del trattamento con ogni singolo dato appreso nel corso della permanenza dell'utente all'interno del *network* (o anche solo ove esso interagisca con *tools* predisposti dal prestatore senza essere registrato o aver effettuato il login[45]), sono varie e difficilmente classificabili, in termini qualitativi, quantitativi e temporali.

Scorrendo le *privacy policies* è possibile affermare che esse – tenute fuori tutte le attività di *disclosure* connesse alle richieste delle autorità competenti – consistano principalmente in: *a*) studio ed elaborazione dei contenuti prodotti e/o visualizzati, delle preferenze, delle azioni e delle interazioni dell'utente ai fini *a*1) del rafforzamento e dell'ampliamento delle relazioni virtuali, *a*2) della comunicazione di suggerimenti pubblicitari, *a*3) dell'implementazione delle stesse informazioni raccolte con maggiori dettagli (ad es. geolocalizzazione + *tagging* in luoghi pubblici, caffè, ristoranti); *b*) miglioramento dei servizi e/o della fidelizzazione dell'utente; *c*) confronto incrociato dei dati personali ricavati dalla piatta-

[43] È lo storico motto di Facebook.

[44] S. Cosimi, *Facebook & co., dall'Oregon alla Svezia: ecco dove sono i data center nel mondo*, in *Repubblica.it*, 6 ottobre 2015.

[45] Una recentissima sentenza della sezione in lingua olandese del Tribunal de première Instance di Bruxelles (9/11/2015), ancora inedita, si sofferma proprio sulla raccolta di informazioni di coloro che non hanno un profilo sui SNs attraverso l'uso dei *tool* «like» e dei tasti di condivisione collocati su siti terzi. La Corte ha intimato a Facebook di interrompere tale attività entro 48 ore dalla pronuncia, pena il pagamento di un'*astreinte* di 250 mila euro al giorno: http://www.privacycommission.be/en/news/judgment-facebook-case/.

forma con quelli forniti da partner commerciali[46]; *d*) trasferimento a siti terzi controllati dalla casa-madre (legame contrattuale o proprietario)[47]; *e*) trasferimento a seguito di contratto di vendita dell'azienda stessa o di una sua controllata[48]; *f*) controllo del rispetto della *netiquette*.

Ogni attività suindicata, oltre che venire espressamente consentita dall'interessato, dovrà rispettare i precetti normativi che regolano le modalità e la durata del trattamento o della conservazione.

La dinamica dei trattamenti occulti dei dati personali, soprattutto nei casi in cui le attività del prestatore si svolgono ad un livello inferiore rispetto a quello di accesso pubblico alle informazioni sul web, è un fenomeno ricorrente e oggetto di studio[49].

Nell'attuale contesto, la questione si arricchisce di nuovi argomenti, di centrale importanza per questa discussione.

[46] Dai termini d'uso di Facebook (13/11/2015): «Riceviamo le informazioni su di te e sulle tue attività all'interno e all'esterno di Facebook da partner terzi, ad esempio le informazioni da parte di un partner quando offriamo servizi congiunti o di un inserzionista sulla tua esperienza e sulle tue interazioni con lui». Dai termini d'uso di Twitter: «richiediamo a fornitori di servizi terzi di svolgere funzioni e di fornirci servizi negli Stati Uniti, in Irlanda e in altri Paesi. Potremmo condividere le tue informazioni personali private con questi soggetti nel rispetto degli obblighi di riservatezza previsti da questa Informativa sulla Privacy e di eventuali altre misure appropriate in materia di riservatezza e sicurezza, a condizione che tali soggetti terzi usino le tue informazioni personali private unicamente per nostro conto e nel rispetto delle nostre istruzioni. Condividiamo le tue Informazioni di pagamento con i provider di servizi a pagamento per elaborare i pagamenti, prevenire, individuare e indagare su frodi e altre attività illecite; facilitare la risoluzione di controversie come i rimborsi o i riaddebiti e per altri scopi legati all'accettazione di carte di credito o di debito. Potremmo comunicare il tuo numero di carta di credito o di debito ai provider di servizi a pagamento o ai circuiti delle carte per monitorare le transazioni tramite carta presso i commercianti e tenere traccia dell'attività di riscossione allo scopo di fornire servizi a pagamento».

[47] Dai termini d'uso di Facebook (13/11/2015): «Condividiamo le informazioni in nostro possesso con le aziende che fanno parte di Facebook. […]».

[48] *Ibidem*: «Se la proprietà o il controllo di tutti o parte dei nostri Servizi o delle relative risorse cambia, potremmo trasferire le tue informazioni al nuovo titolare». Dai termini d'uso di Twitter (13/11/2015): «nel caso in cui Twitter sia coinvolto in una procedura di fallimento, in una fusione, acquisizione, riorganizzazione o vendita dei suoi beni, le tue informazioni potrebbero essere vendute o trasferite nell'ambito della relativa operazione. Quanto stabilito nella presente Informativa sulla Privacy si applicherà alle tue informazioni trasferite al nuovo soggetto. Potremmo divulgare informazioni su di te anche alle nostre società affiliate con lo scopo di contribuire a fornire, personalizzare e migliorare i nostri Servizi e i servizi dei nostri affiliati, tra cui la fornitura di annunci».

[49] Si veda ad. es. A. Mantelero, *Il costo della privacy*, cit., p. 173 ss.; V. Lubello, *Behavioural advertising e la privacy degli androidi*, in O. Pollicino - A.M. Mazzaro, *Tutela del copyright e della privacy sul web: quid iuris*?, Roma, 2012, pp. 239 e ss.

L'approccio qualitativo delle normative comunitarie di settore presuppone che il dato, una volta immesso nella piattaforma, si contraddistingua 'morfologicamente' per elementi che ne permettano *ex ante* la classificazione[50], con la conseguente attribuzione del relativo regime di tutela.

Il consenso, in linea generale, investe preventivamente il tipo di dato immesso ed è valido solo per quelle attività espressamente dichiarate dal responsabile.

I dati personali, trattati in blocchi combinati e combinabili innumerevoli volte, sono forieri di produrre 'nuovo valore' nel senso di correlazioni e risultati utili.

Lo stesso dato anonimo o 'pseudonimizzato', ovvero sottoposto ad un processo di cancellazione di tutti gli elementi astrattamente identificativi, generalmente non protetto dalle norme sulla privacy, fornisce valore aggiunto e, combinato con altri dati anonimi può anche condurre all'identificazione di un soggetto. In altre parole, un *data-set* anonimo, qualora venga sottoposto ad un determinato trattamento, può dar vita a dati nuovi (anche di carattere personale), a loro volta riutilizzabili in maniera impredicibile finchè non si riterranno più utili, ovvero una volta esaurite le tecniche (e le idee) per una loro combinazione[51].

I trattamenti 'secondari' dei dati risultano quindi potenzialmente più importanti in termini economici di quelli primari, con il rischio evidente di elusione ed inefficacia delle normative di settore.

La legge italiana sulla privacy afferma l'importanza che il trattamento non contrasti con i diritti, le libertà e la dignità dell'interessato (art. 1, d.lgs. 196/2003) e venga effettuato soltanto ove necessario (art. 3, d.lgs. cit.), in maniera lecita e secondo correttezza (art. 11, lett. a), d.lgs. cit.).

I dati devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti (art. 11, lett. e), d.lgs. cit.).

Tali regole di condotta poste in capo al responsabile, nonostante siano permeate da principi di portata ampia e flessibile anche *pro futuro* (dignità e compatibilità con i diritti fondamentali), rischiano sovente di rimanere disattesi[52].

Dal punto di vista dei ricavi, le aziende in questione traggono profitto in primo luogo dalle vendite di spazi pubblicitari[53]. Inoltre, la recente

[50] V. ad es., l'art. 4, lett. a) – e), d.lgs. 196/2003.
[51] V. Mayer-Schönberger – K. Cukier, *Big data*, cit., pp. 237 e ss.
[52] S. Rodotà, *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 36 s.
[53] Secondo l'ultimo rapporto trimestrale reso noto agli azionisti, Facebook ha ottenuto

quotazione in borsa influenza sensibilmente il loro valore di mercato. Le attività concernenti il trattamento dei dati si pongono a cavallo tra due settori, poiché foraggiano indirettamente la pubblicità sulle piattaforme e aumentano il patrimonio complessivo dell'impresa stessa, ad esempio in termini di titoli negoziabili (*marketable securities*) o di avviamento (*goodwill*), come d'altronde è stato rilevato dalle autorità giudiziarie: si pensi alla cessione dell'attività imprenditoriale e al connesso valore attribuito ai dati raccolti e trasferiti, spesso solo virtualmente, da un soggetto privato all'altro[54].

4. Nuovi mercati rilevanti e posizioni dominanti tra UE ed USA

Al fine di poter approntare un tentativo di applicazione della normativa antimonopolistica vigente in Europa e negli Stati Uniti alla porzione di mercato in cui operano i *social network*, è opportuno tracciare un breve quadro dei concetti-chiave che ne sostengono l'intera architettura, verificandone ove possibile le evoluzioni interpretative ed applicative.

La normativa *antitrust* comunitaria, inscindibilmente connessa agli obiettivi di promozione di un libero mercato interno competitivo e convergente nei risultati (art. 2 TUE), integra gli strumenti di regolazione *ex ante* e contrasto degli squilibri di mercato con una legislazione settoriale protesa a garantire una tutela trasversale del consumatore, attenta ai suoi bisogni non solo in termini di riduzione dei prezzi o varietà dei prodotti[55].

più del 90% del totale dei ricavi per il terzo trimestre del 2015 dalle pubblicità, di cui il 78% proveniente dal settore mobile. V. *Facebook Reports Third Quarter 2015 Results*, reperibile all'URL: http://investor.fb.com/.

[54] Un esempio paradigmatico è rappresentato dal caso *Toysmart*, in cui un'impresa in crisi della *new economy* dei primi anni 2000 tentò di cedere le banche di dati personali dei propri acquirenti per migliorare la situazione economica. Il caso è citato, unitamente ai suoi estremi, da A. Mantelero, *Attività di impresa in Internet e tutela della persona*, Padova, 2004, p. 152 s. e nota 169. Sul punto v. anche F. Morando – R. Iemma – E. Raiteri, *Privacy evaluation: what empirical research on users' valuation of personal data tells us*, in *Int. Pol'y Rev.*, 2, 2014.

[55] Per un primo quadro v. G. Ghidini, *La concorrenza sleale*, Torino, 2001; A. Frignani – R. Pardolesi, *La concorrenza*, in G. Ajani – A. Benacchio (dir. da), *Tratt. dir. priv. U.E.*, VII, Torino, 2006; M. Libertini, *Principi e concetti fondamentali del diritto antitrust*, in C. Castronovo – S. Mazzamuto, *Manuale di diritto privato europeo*, III, Milano, 2006, pp. 159 ss.; P. Auteri – G. Floridia – V. Mangini – G. Olivieri – M. Ricolfi – P.Spada, *Diritto industriale*, Torino, 2012, pp. 417 e ss.; G. Benacchio, *Diritto privato dell'Unione Europea*, 6ª ed., Padova, 2013, pp. 453 e ss.; S. Vigliar,

Tale strategia bipartita è deducibile dallo stesso Trattato sul funzionamento dell'U.E., che agli artt. 101-109 fissa le regole generali di concorrenza, ampliate nel dettaglio da appositi regolamenti (si vedano ad es. i Regolamenti del Consiglio n. 1/2003 sulle procedure e n. 139/2004 sulle concentrazioni), mentre all'art. 169 dedica un intero (seppur succinto) titolo alla protezione del consumatore: un altro tassello indicativo in tal senso è rappresentato dalla direttiva 2005/29/CE in materia di pratiche commerciali sleali tra imprese e consumatori[56].

Lo sforzo di armonizzazione del legislatore comunitario investe il rapporto tra diritto sovranazionale e municipale e promuove una visione coordinata tra i singoli comparti di tutela (concorrenza, rapporto di consumo, teoria generale del contratto, contratti tipici)[57]: in questa prospettiva dialettica giocano poi un ruolo preminente i diritti fondamentali, in termini declamatori e con riguardo al controllo e all'applicazione giurisprudenziale delle regole.

La vigenza della disciplina concorrenziale è assicurata dalla Commissione, dalla Corte di giustizia e dal Tribunale e, su un diverso livello, dalle Autorità amministrative nazionali competenti (senza dimenticare il ruolo del giudice ordinario)[58], qualora si registrino pratiche imprenditoriali volte a pregiudicare il commercio tra stati membri o tra imprese operanti in uno stesso stato, impedendo, restringendo o falsando 'il gioco della concorrenza'[59].

Il Trattato sul funzionamento dell'Unione riconosce tre fattispecie tipiche, ma sufficientemente 'aperte' di illecito concorrenziale: *a*) gli accordi o le pratiche concordate (art. 101 TFUE), *b*) l'abuso di posizione dominante sul mercato (art. 102 TFUE), *c*) gli aiuti degli Stati membri alle imprese (art. 107 TFUE).

Sull'altra sponda dell'oceano, la più matura disciplina *antitrust* statu-

Antitrust, in M. Colucci – S. Sica, *L'Unione Europea*, Bologna, 2005, pp. 297 e ss.

[56] R. Pardolesi, *La disciplina della concorrenza: uno sguardo d'insieme*, in *La concorrenza e la tutela dell'innovazione*, cit., p. 8; L. Nivarra, *Diritto privato e capitalismo*, Napoli, 2011, p. 97 e ss.

[57] Si veda ad es. A. Somma, *Giustizia sociale e mercato nel diritto europeo dei contratti*, Torino, 2007; C. Castronovo – S. Mazzamuto, *Manuale di diritto privato europeo*, cit., II, pp. 249 e ss.*;* M. Barcellona, *I nuovi controlli sul contenuto del contratto e le forme della sua eterointegrazione: stato e mercato nell'orizzonte europeo*, in *Eur. dir. priv.*, 1, 2008, p. 33 e ss.; P. Stanzione - A. Musio*, La tutela del consumatore*, in M. Bessone (dir. da), *Trattato di diritto privato*, XXX, Torino, 2009.

[58] V. De Luca, *Innovazione tecnologica e concorrenza nello spazio giuridico globale*, in *Riv. dir. comm.*, 7-8, 2004, pp. 891 e ss.

[59] Art. 101 TFUE.

nitense fa capo allo *Sherman Act* del 1890[60], al *Clayton Act* del 1914[61] in materia di concentrazioni, al *Federal Trade Commission Act* (1914)[62] e al *Robinson Patman Act* (1936)[63], che si applica in caso di discriminazione sul prezzo di vendita di prodotti del medesimo grado e tipo di qualità sul territorio americano: autorità competenti in materia a livello federale sono la sezione *antitrust* del *Department of Justice* (DOJ), e il *bureau of competition* della *Federal Trade Commission* (FTC)[64].

In particolare, la sec. 1 dello *Sherman Act* proibisce qualsiasi accordo che limiti in maniera irragionevole il libero commercio, ad esempio concordando i prezzi di un prodotto, riducendone convenzionalmente la produzione, ripartendosi i mercati o rifiutando di contrarre rapporti commerciali con terzi non coinvolti nell'intesa.

La sec. 2, invece, vieta in generale la formazione di monopoli e si estende alle condotte di singole persone fisiche o giuridiche volte a controllare il mercato o a condurre trattative e accordi strumentali a tal fine.

Dotata di un valore di clausola generale è la sec. 5 (a)(1) del FTC *Act*[65] (citato nel corpo della sentenza *Schrems*), per cui è illecito ogni metodo scorretto di concorrenza ed ogni azione o pratica scorrette o ingannevole: per la sua ampiezza essa può abbracciare le fattispecie descritte nelle restanti normative di settore, garantendo astrattamente alla *Federal Trade Commission* competenza su tutte le pratiche distorsive.

Un fattore determinante per la valutazione dei comportamenti anticoncorrenziali di un'impresa è la definizione del 'mercato rilevante' in cui essa opera.

Questa nozione è strettamente connessa a quella di 'prodotto': è quindi necessario individuare quei prodotti che per le loro proprietà, l'uso o il prezzo non siano considerati facilmente interscambiabili dal consumatore[66].

[60] 15 U.S.C. §§ 1-7.
[61] 15 U.S.C. §§ 12–27, 29 U.S.C. §§ 52–53.
[62] 15 U.S.C §§ 41–58.
[63] 15 U.S.C. § 13.
[64] W. Kovacic - P. Mavroidis - D. Neven, *Merger control procedures and institutions: a comparison of the EU and US practice*, Robert Schuman Centre for Advanced Studies, 2014; F. Cengiz, *Antitrust federalism in the EU and the US*, London, 2012; E.M. Fox, *US and EU Competition law. A Comparison*, in E.M. Graham - J. D.Richardson (a cura di), *Global Competition Policy*, Washington, 1997, pp. 339 e ss.
[65] 15 U.S.C. § 45(a)(1): «Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful. […]».
[66] A. Frignani – R. Pardolesi, *Fonti fini e nozioni generali di diritto della concorrenza nella CE*, in *La concorrenza*, cit., p. 15.

Il *relevant product market* viene costruito sulla base di parametri materiali, spaziali e temporali, abbracciando ogni tipologia di relazione che si crea intorno ad un medesimo prodotto[67] e valorizza la percezione soggettiva del consumatore: l'analisi del mercato è difatti basata sulla domanda e mira in senso più ampio a verificare l'impatto di una determinata condotta sui benefici ricavati dal consumatore[68].

Una volta definito il mercato di riferimento, sarà necessario calcolare le sue quote e il potere attribuibile ad una data impresa (*market power*), adottando caso per caso parametri specifici e funzionali, variabili in base alla tipologia di consumatore (anziano, bambino, adulto) o di prodotto e ancora rispetto ad ogni singola ipotesi di divieto *antitrust* (abuso di posizione dominante, concentrazione, intesa restrittiva).

Secondo la Commissione, l'incremento del potere di mercato consiste «(nel)la possibilità per una o più imprese di aumentare i prezzi, ridurre la produzione, la scelta o la qualità dei beni e servizi, diminuire l'innovazione o influenzare in altro modo i parametri di concorrenza per ricavarne un vantaggio» [69].

La casistica *antitrust* nel mercato dei servizi in Internet si caratterizza per la lunga durata dei procedimenti, il sincronico coinvolgimento delle autorità comunitarie e di quelle statunitensi e per gli esiti sovente favorevoli alle imprese oggetto di indagine.

Nel caso *Google/Doubleclick*[70], l'acquisizione da parte del motore di ricerca generalista di una società che fornisce tecnologie di collocamento di messaggi pubblicitari attraverso servizi di tracciamento (ad es. con i c.d. *cookies*), è stata approvata sia dalla FTC che dalla Commissione, sulla base della normativa sulle concentrazioni.

In ambito europeo, il regolamento n. 139/2004 si applica a tutte le

[67] È il caso del già citato 'mercato a più versanti': M. Granieri, *Two-sided markets and the credit card industry: are antitrust authorities missing the big picture?*, *Law & Economics Working Paper*, 2011, (www.law-economics.net); M. Colangelo – V. Zeno-Zencovich, *La intermediazione on-line e la disciplina della concorrenza*, cit., p. 53 s.; A. Frignani – R. Pardolesi, *Fonti, fini e nozioni generali*, cit., p. 19.

[68] M. Libertini, *Principi e concetti fondamentali del diritto antitrust*, cit., p. 165 ss.

[69] Commissione europea, *Orientamenti relativi alla valutazione delle concentrazioni orizzontali a norma del regolamento del Consiglio relativo al controllo delle concentrazioni tra imprese*, in *GUUE*, C 31, 5 febbraio 2004, pp. 5–18.

[70] FTC, *Google/DoubleClick*, FTC File No. 071-0170 (Dec. 20, 2007), disp. all'URL: http://www.ftc.gov/os/caselist/0710170/071220statement.pdf/; Commissione europea, decisione 11 marzo 2008, Caso COMP/M.4731 — *Google/DoubleClick*, C(2008) 927 final.

concentrazioni di dimensione comunitaria[71] che producono una modifica duratura del controllo sul mercato unico, «in funzione della loro incidenza sulla struttura della concorrenza» (considerando 6).

L'impatto anticompetitivo della concentrazione va verificato anche guardando ai principi generali sull'abuso di posizione dominante ex art. 102 TFUE e quindi alla capacità di una data impresa di determinare i prezzi e controllare la produzione in un determinato mercato, attraverso: *i*) comportamenti volti ad escludere i concorrenti con mezzi diversi dalla competizione basata sui meriti dei prodotti o dei servizi forniti (accordi di esclusiva, vendite abbinate o aggregate, comportamenti predatori, rifiuto ad effettuare forniture)[72] o *ii*) preclusioni anticoncorrenziali in danno dei consumatori, quali l'aumento ingiustificato dei prezzi[73].

Nel caso di specie, il mercato di riferimento è stato identificato con quello dell'*on-line advertising* (fornitura di spazi pubblicitari per *Google* e collocamento di inserzioni per *Doubleclick*) e segmentato in base alla tipologia di comunicazione commerciale veicolata (per *Google*)[74] e al tipo di contraente (distinzione tra inserzionisti o editori per *Doubleclick*).

La definizione di mercato rilevante non è stata però affermata in via assoluta, ma tenuta aperta a future evoluzioni interpretative[75].

Rispetto a tali indici, l'acquisizione di *Doubleclick* è stata ammessa sia sotto un profilo orizzontale (concorrenza tra i due operatori), sia verticale (concorrenza dei due distinti operatori sui mercati in cui operano, ovvero il collocamento per le inserzioni pubblicitarie per *Doubleclick* e la pubblicità collegata alle ricerche e i servizi di intermediazione di inserzioni pubblicitarie per *Google*).

Inoltre, FTC e Commissione si sono soffermate sul possibile effetto anticompetitivo sortito dalla combinazione delle banche dati delle due

[71] Reg. n. 139/2004, art. 1, n. 2 e 3.

[72] V. Commissione europea, *Orientamenti sulle priorità della Commissione nell'applicazione dell'articolo 82 del trattato CE al comportamento abusivo delle imprese dominanti volto all'esclusione dei concorrenti*, 2009/C 45/02, in *GUUE*, C 45/7, 24 febbraio 2009.

[73] Rileva la dottrina che, differentemente l'ordinamento americano non ritiene, in generale, incompatibile con i principi della concorrenza la libertà di determinare il prezzo che massimizzi il profitto: A. Frignani, *L'abuso di posizione dominante,* in *La concorrenza*, cit., p. 202.

[74] Inserzioni testuali e non testuali, anche illustrate e collegate o meno alle ricerche o ai vari canali di vendita diretta e/o tramite reti e scambi di inserzioni pubblicitarie.

[75] FTC, *Google/DoubleClick*, cit., p. 13: «The markets within the online advertising space continue to quickly evolve, and predicting their future course is not a simple task. Accounting for the dynamic nature of an industry requires solid grounding in facts and the careful application of tested antitrust analysis».

imprese. A causa dei vincoli contrattuali intercorrenti tra *Doubleclick* e i propri clienti, i *data-set* non si sarebbero prestati ad un 'uso incrociato', essendo fruibili soltanto dall'inserzionista che ha proposto l'annuncio pubblicitario all'utente in visita alla pagina web[76].

Ad ogni modo, a seguito della concentrazione, tale complesso di dati non avrebbe rappresentato un input decisivo atto a determinare un vantaggio sul mercato di riferimento[77], posto anche che tutti i concorrenti di *Google* avevano già integrato nei propri portali le tecnologie in questione.

Le motivazioni proposte dalle due autorità – risalenti a quasi dieci anni or sono – nascondono alcuni limiti: il mercato rilevante è inquadrato soltanto sotto il profilo delle vendite pubblicitarie e le giustificazioni addotte per 'sminuire' il potere di mercato connesso alla fusione dei *data-set* sono messe in discussione dalle prassi contrattuali che coinvolgono utente e prestatore.

Le clausole predisposte dai maggiori *social media* riconoscono esplicitamente, come si è avuto modo di rilevare, un utilizzo alternativo e incrociato dei dati personali o anonimi degli utenti che hanno avuto accesso alla piattaforma.

Inoltre, la prospettiva adottata dalla Commissione è esclusivamente di tipo qualitativo: essa valuta il 'dato' oggetto di trattamento come

[76] FTC, Google/DoubleClick, cit., p. 12: «[…] However, the customer and competitor information that DoubleClick collects currently belongs to publishers, not DoubleClick. Restrictions in DoubleClick's contracts with its customers, which those customers insisted on, protect that information from disclosure, and we understand that Google has committed to the sanctity of those contracts. Furthermore, if, post-transaction, Google were to change or breach those contracts, the evidence does not support the conclusion that the aggregation of consumer or competitive information accessible to Google as a result of its acquisition of DoubleClick is likely to confer market power. The evidence, for instance, does not support the suggestion that Google would be able to use competitively sensitive information in DFP – particularly pricing information – to disadvantage its ad intermediation competitors. […]». Commissione europea, Google/DoubleClick, cit., par. 361:«The notifying party submitted that DoubleClick's current contracts with advertisers do not allow the use of data regarding which web pages a user visited, in order to better target ads from other advertisers than those that were instrumental in bringing this data into existence, that is to say, the advertiser that had served an ad to the user when the user was visiting the web page. By extension, the merged entity would also be contractually prevented from using that part of its enlarged database originating from DoubleClick to improve, for example, targeting of search ads on Google's sites or contextual ads in the AdSense network. […]».

[77] FTC, *Google/DoubleClick*, cit., p. 12: «[…] Yet, the evidence indicates that neither the data available to Google, nor the data available to DoubleClick, constitutes an essential input to a successful online advertising product. […]»;Commissione europea, *Google/DoubleClick*, cit., par. 365.

un'informazione precisa che può servire solo al singolo inserzionista per modulare una determinata offerta[78], senza tenere in considerazione che i nuovi sistemi di trattamento traggono indicazioni fondamentali (e relativo plusvalore) finanche dalla quantità di dati raccolti ed elaborati.

Nel successivo caso *TomTom/Tele Atlas*[79], la Commissione ha esplorato l'integrazione verticale tra un'azienda produttrice di *software* e *hardware* per la navigazione GPS e un'altra fornitrice di mappe digitali.

Dalle risultanze dell'indagine è emersa l'importanza di proteggere il grado di 'confidenzialità' delle informazioni prodotte dagli utilizzatori delle mappe di *Tele Atlas* e passibili di acquisizione.

La prospettiva di una 'migrazione' di utenti verso un'impresa concorrente ha attribuito all'aspettativa di privacy un valore che influenza direttamente il potere di mercato dell'impresa in predicato di essere assorbita, con effetti paragonabili a quelli di degradazione del prodotto[80].

In *Microsoft/Yahoo*[81], sia la Commissione che il DOJ hanno reputato ammissibile la commistione tra servizi di ricerca e servizi pubblicitari

[78] Commissione europea, *Google/DoubleClick*, cit., par. 362:«[…] advertisers have no interest in other advertisers having access to their data and thus getting insight into competitively important information such as information about the pricing of ads across different websites. Given this probable lack of *ability* to force a change in contractual relations, it is also doubtful whether DoubleClick would have an incentive to try to do so since stopping to be a neutral service provider might prompt customers to switch over. […]»

[79] Commissione europea, decisione 14 maggio 2008, Caso COMP/M.4854 — *TomTom/Tele Atlas*, C(2008) 1859.

[80] Commissione europea, *TomTom/Tele Atlas*, cit., par. 273 s.: «[…] Therefore it has to be examined whether the incentive to protect its customers' confidential information would change post-merger, should the merged company be in a position to obtain confidential information from its customers. The Commission's analysis reveals that Tele Atlas would have incentives to keep its current customers from switching to NAVTEQ, since losing a customer would not be compensated by sufficient additional gains downstream independently of whether NAVTEQ significantly raised its prices. The market investigation showed that in this case confidentiality concerns can be considered as similar to product degradation in that the perceived value of the map for PND manufacturers would be lower if they feared that their confidential information could be revealed to TomTom. As a consequence, Tele Atlas's map database could be perceived as relatively less valuable than NAVTEQ's map database. Confidentiality concerns could thus lead Tele Atlas's customers to consider switching to NAVTEQ. […]».

[81] U.S. Department of Justice, *Statement of the Department of Justice Antitrust Division on Its Decision to Close Its Investigation of the Internet Search and Paid Search Advertising Agreement Between Microsoft Corporation and Yahoo! Inc.*, 18 febbraio 2010, reperibile all'URL: http://www.justice.gov/atr/public/press_releases/2010/255377.pdf/; Commissione europea, decisione 18 febbraio 2010, Caso COMP/M.5727 - *Microsoft/Yahoo/Search Business*, C(2010) 1077..

offerti a pagamento agli inserzionisti da entrambe le imprese. La possibilità di poter entrare in competizione con *Google* in entrambi i mercati giustificava la concentrazione.

Il fattore procompetitivo è stato individuato proprio nell'acquisizione di un vasto set di dati attinenti le *queries*[82], che avrebbe favorito i due motori di ricerca (*Bing!* e *Yahoo*) sul piano dell'innovazione[83].

Più di recente, le autorità competenti si sono misurate con alcune acquisizioni condotte da *social network*.

In *Facebook/Whatsapp*[84], la Commissione ha considerato tre mercati rilevanti: i servizi di comunicazione tra consumatori, quelli di *social networking* e l'*on-line advertising*.

Con riferimento a quest'ultimo mercato, si è constatato come in quel tempo non fosse prassi di *Facebook* quella di cedere i dati raccolti agli inserzionisti o a terzi come 'prodotto nuovo e diverso' dal servizio di *advertising*[85]. Dall'altra parte, *Whatsapp* non conservava i dati delle conversazioni (non fungibili per scopi di *advertising*) sui propri server, poiché stoccati unicamente nei dispositivi mobili degli utenti o nelle *cloud* agli stessi riconducibili[86].

Ad ogni modo, la concentrazione avrebbe comportato la raccolta da parte di *Facebook* dei dati personali degli utenti *Whatsapp*: tale conseguenza è stata in astratto valutata come non conveniente per l'impresa controllata, riconoscendo implicitamente il peso dell'aspettativa di *privacy* dei consumatori ai fini della scelta sull'utilizzo di un dato servizio di

[82] U.S. Department of Justice, *Statement*, cit.: «[…] because it will have access to a larger set of queries, which should accelerate the automated learning of Microsoft's search and paid search algorithms and enhance Microsoft's ability to serve more relevant search results and paid search listings, particularly with respect to rare or «tail» queries. The increased queries received by the combined operation will further provide Microsoft with a much larger pool of data than it currently has or is likely to obtain without this transaction. This larger data pool may enable more effective testing and thus more rapid innovation of potential new search-related products, changes in the presentation of search results and paid search listings, other changes in the user interface, and changes in the search or paid search algorithms. This enhanced performance, if realized, should exert correspondingly greater competitive pressure in the marketplace […]».

[83] Commissione europea, *Microsoft/ Yahoo/Search Business*, cit., par. 223: «[…] Furthermore, as submitted by the notifying party and as analysed above, the effects of scale are likely to allow the merged entity to run more tests and experiments on the algorithm in order to improve its relevance. […]».

[84] Commissione europea, decisione 3 ottobre 2014, Caso COMP/M.7217 - *Facebook/ Whatsapp*, C(2014) 7239 final.

[85] In definitiva analogamente a quanto affermato in *Google/Doubleclick*.

[86] Commissione europea, *Facebook/Whatsap*, cit., par. 70 s.

comunicazione multi-piattaforma[87].

Nel caso di specie, il potere di raccolta dei dati sul mercato pubblicitario derivante dalla concentrazione non sarebbe cresciuto in maniera lesiva della concorrenza, in ragione della presenza di un numero consistente di imprese nel settore di riferimento: la quota percentuale di dati controllati da *Facebook* avrebbe valicato la soglia del 9% globale registrato nel 2013, lasciando ancora una grossa 'fetta della torta' nelle mani di terzi[88].

I casi analizzati evidenziano come spesso la nozione di 'mercato rilevante' sia stata apprestata privilegiando l'attività di *advertising*, fonte dei maggiori profitti dichiarati.

La percezione dell'importanza della raccolta dei dati è via via cresciuta negli interpreti, slegandosi a volte dalla mera logica dell'uso per fini pubblicitari (*TomTom/Tele Atlas*; *Facebook/Whatsapp*).

Alla luce degli elementi sin qui raccolti, è possibile approcciare alla nozione di mercato rilevante nei *social network* da tre differenti angoli visuali: *a*) il servizio reso all'utente, nelle sue molteplici declinazioni; *b*) le tipologie di *advertising* vendute agli operatori commerciali; *c*) l'attività di trattamento dei dati, che coinvolge e può influenzare sia *a*) che *b*), ma invero valica anche questa concezione restrittiva affermandosi come autonomo 'prodotto'[89].

Ci si concentri ad esempio *a*1) sull'opportunità che gli utenti possano scegliere dei servizi analoghi ma maggiormente attenti al profilo della privacy (nel senso quindi della possibilità di accedere ad un servizio qualitativamente migliore), *b*1) sulle attività commerciali di *profiling* e *beavihoural*

[87] *Ibidem*, par.186: «As regards the incentive of the merged entity to start collecting data from WhatsApp users (for example, age, gender, country, message content), a number of respondents pointed out that, if the merged entity were to do so, this may prompt some users to switch to different consumer communications apps that they perceive as less intrusive.106 Moreover, the Commission notes that, as explained above (174), the need to abandon WhatsApp's plan for […] may reduce Facebook's incentive to start collecting data from WhatsApp messages».

[88] *Ibidem*, par.188. Secondo le stime, il 33% spetterebbe a Google, mentre il 58, 67% sarebbe suddiviso tra imprese minori.

[89] Sul punto, la dottrina si assesta su posizione differenti: il dibattito è cresciuto, soprattutto in ambito extra-UE. V. G. Rossi, *Social network e diritto antitrust*, in *AIDA*, 2011, pp. 77 e ss.; E. Camilleri, *«Facebook credits» e commercializzazione di beni virtuali per social games: l'abuso di posizione dominante alla prova di un mercato con piattaforma plurilaterale*, *ivi*, pp. 144 e ss.; P. Jones Harbour – T.I. Koslov, *Section 2 In A Web 2.0 World: An Expanded Vision Of Relevant Product Markets*, in 76 *Antitrust L. J.* 769 (2011); C. Tucker – A. Marthews, *Social networks, Advertising and Antitrust*, in 19 *Geo. Mason L. Rev.* 1211 (2012); M.K. Ohlhausen – A.P. Okuliar, *Competition, Consumer Protection, And The Right [Approach]* To Privacy, in 80 *Antitrust L. J.* 121 (2015).

advertising alimentate dalla raccolta di dati, *c*1) sul valore intrinseco dei dati stoccati e conservati dal prestatore.

Sotto questo ultimo profilo, tali attività sono precondizione di nuovi ed indefiniti trattamenti, rappresentando per certi versi un'attività diversa da quella per cui si è prestato il consenso[90] e configurando un differente mercato rilevante avente come oggetto un servizio non sostituibile, nel senso di [*c* 1) ≠ *b*) e *a*)].

Volendo adottare tale ampia e flessibile nozione di mercato rilevante, la disponibilità, presente e futura di *data-set* personali ed anonimi, potrebbe essere valutata almeno in tre modi:

[*a*) + *b*)]: La celerità dei meccanismi di registrazione alla piattaforma non è adeguatamente bilanciata con strumenti di estrazione e trasferimento dei dati personali che permettano all'utente di spostarsi da un servizio di *social networking* all'altro[91].

Ad esempio, l'impossibilità di esportare l'insieme dei contenuti connessi ai legami di amicizia virtuale (dagli indirizzi e-mail cui fanno capo sino a conversazioni e foto), impedirebbe agli utenti di scegliere se prendere parte, alternativamente o cumulativamente, a reti sociali che ad esempio non effettuano la raccolta e il trattamento dei dati personali per fini commerciali[92].

Ancora, si guardi alla facoltà di spostare il proprio patrimonio di immagini su piattaforme specializzate o di esercitare liberamente il diritto all'anonimato, dalla giurisprudenza affermato come «immanente in Internet»[93] e invero spesso negato da pratiche che costringono gli utenti ad identificarsi con nomi reali (c.d. *Nymwar*).

Tali vincoli agirebbero da barriere di accesso per consumatori e concorrenti sul mercato dei servizi di *social networking* e di *advertising*, con un effetto vicino, a livello concettuale, al diniego opposto da *Microsoft* a fornire informazioni indispensabili per l'interoperabilità tra *Windows* e altri sistemi operativi, censurato in più occasioni dalla Commissione e dal

[90] Sul punto ad es. S.D. Seybold, *Somebody's Watching Me: a Civilian Oversight of Data-Collection Technologies*, in 93 *Tex. L. Rev.* 1029 (2015), spec. p. 1035.

[91] E. Camilleri, *«Facebook credits»*, cit., p.155.

[92] Alcuna dottrina prospetta ancora la configurabilità di «un abuso di dipendenza economica per interruzione arbitraria delle relazioni commerciali in atto da parte del gestore a fronte di un utente professionista che abbia riposto nel social network dati e contatti indispensabili all'esercizio dell'attività economica e che li perda senza preavviso». Così M. Granieri, *Le clausole ricorrenti nei contratti dei social networks dal punto di vista della disciplina consumeristica dell'Unione europea*, cit., p. 139.

[93] BGH, 23 settembre 2014 – VI ZR 358/13, in *Dir. Inf.* 2015, p 169 ss.

Tribunale di primo grado[94].

L'informazione creata dall'utente è sottoposta ad un regime legale e tecnico di *enclosure* connesso all'architettura in cui lo stesso si muove[95].

Nel caso *Microsoft* – come d'altronde nel recente caso *Google search*[96]– la necessità di garantire l'interoperabilità è stata affermata sulla base della *essential facility doctrine*.

La barriera in entrata equivarrebbe a un rifiuto di accesso ad un'infrastruttura essenziale: tale eccessiva estensione del concetto di *essential facility*, prima circoscritto a porti, aeroporti, reti elettriche o di comunicazione, è sottoposta a costanti critiche da parte della dottrina[97].

In questo caso, invece, l'oggetto dell'istanza non è un codice sorgente o un *software* (sistema operativo o algoritmo) e, più in generale una peculiarità della piattaforma che conchiude in termini di innovazione l'essenza del servizio stesso nonchè la sua diversità ed appetibilità, ma coincide con le pure e singole informazioni apprese dal prestatore, siano esse personali che anonime.

La titolarità dei diritti di autodeterminazione o privativa sui contenuti riconosciuta all'utente dalle condizioni d'uso e dalle leggi, conferma la genuinità di una pretesa di interoperabilità e controllo delle informazioni, anche ai fini di una fuoriuscita dalla piattaforma stessa.

[94] Commissione europea, decisione 24 marzo 2004 n. 2007/53/CE, caso COMP/C-3/37.792 – *Microsoft*, in *GUUE*, L 32, 2007, pp. 23 e ss.; Tribunale primo grado UE, 17 settembre 2007, caso *Microsoft/Commissione* (T-201/04), in *Foro it.*, 2008, IV, 114 (solo mass.), n. R. Pardolesi – G. Colangelo; Tribunale UE (Seconda Sezione), 27 giugno 2012, Microsoft/Commissione (T-167/08), in *Racc.*, 2012, p. 3232 e ss.La vicenda aveva in primo luogo coinvolto gli Stati Uniti, rappresentando in definitiva un unico, grande *leading case* in tema di concorrenza in Internet: *United States v. Microsoft Corp.,* 84 F. Supp. 2d 9, 20 (D.D.C. 1999); *Massachusetts v. Microsoft Corp*., 373 F.3d 1199, 1226 (D.C. Cir. 2004). La casistica su Microsoft comprende altresì alcune decisioni concernenti l'installazione seriale sui sistemi operativi Windows di browser Internet quali I. Explorer o Netscape: Commissione europea, decisione 16 dicembre 2009, Caso COMP/C-3/39.530 – *Microsoft (tying)*, *United States v. Microsoft Corporation,* 253 F.3d 34 (D.C. Cir. 2001).

[95] Tale situazione è stata da alcuni paragonata al rifiuto di accesso ad un'infrastruttura o un servizio essenziale: European Data Protection Supervisor, *Privacy and competitiveness in the age of big data*, cit., p. 30 s.

[96] V. FTC*, In the manner of Motorola Mobility LLC, and Google Inc.*, Docket No. C-4410 (14/07/2013). Per seguire l'iter quinquennale (ancora non concluso) d'indagine della Commissione si consulti l'URL: http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=1_39740/..

[97] Per tutti v. R. Pardolesi, *«Googlelaw».Del ricorso alla disciplina antitrust per colpire il tiranno benevolente*, in Foro it., 2013, V, 18 e M. Lao, *«Neutral» Search As A Basis for Antitrust Action?, in Harv. J. of L. & Tech.Occasional Paper Series — July 2013.*

Si potrebbe obiettare che i consumatori non sono costretti a rimanere nella piattaforma e lo fanno solo perché si tratta di un servizio qualitativamente superiore e di successo o, ancora perché spinti dalla *path dependence*[98]: la visione 'datacentrica' del mercato dei servizi di *social networking*, confermata dall'esistenza di operatori più piccoli e già in grado di soddisfare tali richieste[99], suggerisce quantomeno una possibile verifica in termini di dominanza di tali scenari[100].

[*a*) + *b*) + *c*)]: Il trasferimento e la concentrazione di *data-set* sottrarrebbe alle imprese concorrenti l'accesso a contenuti indispensabili (si pensi alla lista di utenti di *Whatsapp*, inglobati nel servizio *Facebook*), alla stregua della cessione di un'ampia libreria di brani musicali.

Nel caso *AOL/Time Warner*[101], la Commissione ha sostenuto che il controllo di un catalogo musicale di grandi dimensioni può garantire 'un potere di mercato sostanziale', consistente ad esempio nel rifiuto di concedere i propri diritti o la minaccia di non concederli, oppure l'imposizione di prezzi elevati o discriminatori, o altre condizioni commerciali non eque ai propri clienti desiderosi di acquisire tali diritti[102].

A livello operazionale, una banca dati di brani musicali digitali protetti da diritti d'autore agli inizi degli anni 2000, può essere comparata in termini di portata proprietaria e prospettive di sfruttamento ed appetibilità al consumo (*must-stock product*)[103] all'insieme di dati personali utilizzabili separatamente e sincronicamente per scopi pubblicitari, di fidelizzazione dell'utente o di accumulo del 2015[104], con analoghi effetti di *foreclosure*[105].

[98] G. Rossi, *Social network e diritto antitrust*, cit., p. 87 s.

[99] Nel campo dei social network si segnalano ad esempio UmeNow e Sgrouples, mentre per i motori di ricerca esistono servizi quali DuckDuckGo.

[100] P. Jones Harbour – T.I. Koslov, *Section 2 In A Web 2.0 World: An Expanded Vision Of Relevant Product Markets*, cit., p. 790 s.; C. Tucker – A. Marthews, *Social networks, Advertising and Antitrust*, cit., p. 1211 ss.

[101] Commissione europea, decisione 11 ottobre 2000, caso n. 2001/718/CE - *AOL/Time Warner*, in GUCE., L 268, 9 ottobre 2001, pp. 28 ss.

[102] *Ibidem*, par. 47.

[103] Sul punto v. Commissione europea, 13 maggio 2009, Caso COMP/C-3/37.990 — *Intel*, 2009/C 227/07.

[104] Alcuni rilievi sul progressivo avvicinamento tra le due categorie in termini rimediali sono proposti, seppur in maniera differente da G. Resta, *Anonimato, responsabilità, identificazione: prospettive di diritto comparato, in Dir. Inf.* 2014, p. 199 s.; V. Mayer-Schönberger – K. Cukier, Big data, cit., pp. 233 ss.

[105] Sul punto v. anche Commissione europea, decisione del 13 ottobre 2000, Caso COMP/M.2050 - *Vivendi / Canal+ /Seagram*, in *GUCE*., C 311, pp. 3 e ss., citata da G. Rossi, *Cyber-antitrust*, cit., pp. 269 e ss., cui si rimanda per le interessanti conclusioni proposte. Per una rassegna degli altri precedenti negli Stati Uniti si rimanda alla disa-

Si deve aggiungere che i *data-set* hanno un valore d'uso e di scambio[106] che varia rispetto al numero di singoli atti di sfruttamento autorizzati dal soggetto titolare dell'esclusiva (ad es., la vendita e l'ascolto di un brano musicale), ma sopratutto cresce in maniera esponenziale parallelamente all'indefinita possibilità di combinazioni cui si prestano le informazioni raccolte nell'era della 'datizzazione'[107].

Il 'dato', in definitiva, rappresenta la fonte dei molteplici input cui deve essere ricondotta ogni relazione rilevante ai fini della definizione del mercato.

- [*a*) + *c*)]: Inquadrata la pretesa di privacy dell'utente come una legittima aspirazione di miglioramento del servizio, l'analisi si sposta sul concorso tra tutela dei dati personali e disciplina consumeristica in tema di consenso, accettazione espressa e contenuto delle clausole di utilizzo[108].

L'analisi dei termini d'uso dei maggiori SNs denota ancora un'opacità delle informazioni sui trattamenti che pone dubbi sulla genuinità della raccolta del consenso dell'utente e in termini paracontrattuali sull'eccessivo squilibrio del sinallagma[109].

Indicativi in tal senso appaiono i recenti ordini con cui la FTC ha imposto ai maggiori *social media* obblighi di trasparenza e diligenza nella raccolta, conservazione e trattamento dei dati personali degli utenti, constatando altresì la violazione dei *safe harbor principles*[110].

---

mina offerta da v. P. Jones Harbour – T.I. Koslov, *Section 2 In A Web 2.0 World: An Expanded Vision Of Relevant Product Markets*, cit., pp. 787-792.

[106] È infatti fondamentale comprendere come le due prospettive si incrocino: ogni dato, combinato e correlato ad altri, può rappresentare un autonomo risultato in termini di valore d'uso e, conseguentemente un diverso profitto per chi lo sfrutta ed utilizza sotto forma di merce. V. J. Eaton, *Economia Politica*, cit., pp. 29 e ss.

[107] Trattandosi di beni 'non competitivi': V. Mayer-Schönberger – K. Cukier, *Big data*, cit., p. 139.

[108] Si è affrontato l'argomento in S. Sica – G. Giannone Codiglione, *I social network sites e il 'labirinto' delle responsabilità*, cit., spec. p. 2716 ss. e ivi ampia bibliografia citata.

[109] Del resto, la gratuità 'interessata' o 'mascherata', dei servizi di *social networking* non rientra ad alcun titolo entro il classico schema gratuità/liberalità: «l'assenza di un sacrificio economico immediato non è affatto indice di uno spirito di liberalità e può essere, invece, perfino interno ad una logica dello scambio patrimoniale che domina tutta la materia dei rapporti sociali ed economici nel sistema dei codici civili». A. Galasso – S. Mazzarese (a cura di), *Il principio di gratuità*, Milano, 2008, p. 496.

[110] Cfr. FTC, *In the Matter of Twitter, Inc.*, File No. 092 3093 (March 3, 2011); *In the Matter of Google, Inc.,* File No. 102 3136 (Oct. 13, 2011); *In the Matter of Myspace, LLC*, File No. 102 3058 (Aug. 30, 2012); *In the Matter of Facebook, Inc.*, File No. 092 3184 (July 27, 2012), p. 4: «[…] IT IS ORDERED that Respondent and its representatives, in

5. Convergenza dei rimedi e neutralità della rete

Di là del tecnicismo della materia e delle connesse difficoltà applicative dovute, in primo luogo, alle diverse accezioni di 'mercato' e 'libertà d'impresa' su cui può fondarsi un'opinione sul punto, lo studio delle regole antimonopolistiche nello spettro della preminenza, in linea di principio, del diritto fondamentale alla tutela dei dati personali sull'interesse economico dei gestori e sul connesso interesse pubblico all'accesso alle informazioni, fornisce indicazioni sull'efficienza e l'effettività delle diverse tutele meritevoli di futuri approfondimenti[111].

Un'implicita conferma sull'inizio di un (difficile) processo di convergenza dei rimedi sembra giungere dalla bozza di Regolamento europeo sulla tutela dei dati personali e, ad un diverso livello, dai recenti interventi normativi che hanno interessato, prima negli Stati Uniti e poi in Europa, la c.d. neutralità della rete[112].

Nell'ultima bozza del Regolamento privacy, approvata dal Consiglio d'Europa l'11 giugno 2015[113], all'art. 6, n. 3 bis, la liceità del trattamento viene valutata anche con riguardo ad 'ulteriori trattamenti'. In questo senso, il considerando 23 aggiunge che è *«necessario applicare i principi di protezione dei dati a tutte le informazioni relative ad una persona fisica identificata o identificabile. I dati, compresi i dati pseudonimizzati, che potrebbero essere attribuiti ad una persona fisica dall'utilizzo di ulteriori informazioni, dovrebbero essere considerati come informazioni su una persona fisica identificabile* […]».

---

connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information,including, but not limited to: […]the extent to which Respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or any third party, including, but not limited to, the U.S.-EU Safe Harbor Framework. […]». Tutta la documentazione sui casi è reperibile all'URL: http://www.ftc.gov/. Per una disamina delle decisioni più significative v. S. Sica – V. D'Antonio, I Safe Harbour privacy Principles: genesi, contenuti, criticità, in questo Volume par. 4.

[111] V. ad es. J.C. Cooper, *Privacy And Antitrust: Underpants Gnomes, The First Amendment, And Subjectivity*, in 20 *Geo. Mason L. Rev.* 1129 (2013), spec. p. 1146.

[112] T. Wu, *Network Neutrality, Broadband Discrimination* in *J. on Telecomm. & High Tech. L.*, 2003, p. 141 ss., 2003; S. Sica – V. Zeno-Zencovich, *Manuale di diritto dell'informazione e della comunicazion*e, cit., pp. 351 e ss.

[113] Il testo del regolamento è disponibile all'URL: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/it/pdf/.

All'art. 18, si stabilisce poi un nuovo ed autonomo diritto alla portabilità dei dati personali immessi sulle piattaforme[114], che segue l'art. 17 sul «diritto alla cancellazione e all'oblio» e il 17 *bis* sulla «limitazione di trattamento».

L'*Open Internet order* della *Federal Communicatio Commission* e il Regolamento riguardante «il mercato unico europeo delle comunicazioni elettroniche e per realizzare un continente connesso», approvato ed in attesa di firma, reintroducono e consolidano principi e regole atte a promuovere la crescita di una rete veloce, imparziale e aperta (*fast, fair and open network*).

L'ordine del 26 febbraio 2015[115], rappresenta una conseguenza della sentenza *Verizon v. FCC*[116]: la nuova regolamentazione estende il proprio ambito d'applicazione ad ogni tipo di servizio a banda larga, mobile o fisso e riclassifica l'accesso ad Internet come servizio di telecomunicazione e non più come mero servizio informativo, equiparandolo ad un bene di utilità primaria a rilevanza pubblica come il telefono (c.d. *common carrier*)[117].

Le regole dell'*Open Internet order* (*bright line rules*) investono il gestore della rete con il divieto di bloccare l'accesso a contenuti leciti, applicazioni, servizi, o dispositivi non dannosi (*no blocking*); ridurre o degradare il traffico Internet legale sulla base di contenuti, applicazioni, servizi o

[114] «L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile a macchina i dati personali che lo riguardano forniti ad un responsabile del trattamento e ha il diritto di trasmettere tali dati a un altro responsabile del trattamento senza impedimenti da parte del responsabile del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a) o dell'articolo 9, paragrafo 2, lettera a) o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati.2 bis. L'esercizio di tale diritto lascia impregiudicato l'articolo 17. Il diritto di cui al paragrafo 2 non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento. 2 bis bis. Il diritto di cui al paragrafo 2 non si applica se la divulgazione di dati personali viola i diritti di proprietà intellettuali relativamente al trattamento di tali dati personali».

[115] FCC, *In the Matter of Protecting and Promoting the Open Internet*, Docket No. 14-28, 12 marzo 2015. Un interessante commento dell'*order* è stato redatto da un gruppo di esperti coordinato dal prof. M. Dècina, in seno al MISE, nel corso della discussione in Consiglio del Regolamento europeo: Aa.Vv., *Riflessioni sull'Open Internet Order della FCC*, reperibile all'URL: http://www.sviluppoeconomico.gov.it/images/stories/documenti/Open_internet.pdf/.

[116] 740 F.3d 623 (D.C. Cir. 2014).

[117] Il richiamo è sopratutto al Title II del *Communications Act* e ancora alla sec. 706 del *Telecommunications Act of* 1996.

dispositivi non dannosi (*no throttling*) ed offrire a pagamento particolari servizi di traffico Internet rispetto ad altri (*no paid priorization*), creando disparità di connessione alla Rete attraverso l'offerta di *fast lanes*[118].

Fondamentale appare inoltre il princìpio di «no unreasonable interference or disadvantage to consumers or edge providers», che modula l'azione regolatoria più in generale attorno agli interessi dell'utente e dei prestatori di servizi web. L'*order* ammette in astratto che anche l'*edge provider* (quale un *social network*) possa offrire ai propri utenti servizi differenziati di tipo *premium*, a patto che venga rispettata la regola di non produrre un'irragionevole o svantaggio nei confronti di tutti gli altri consumatori o concorrenti[119].

La nozione comunitaria di 'neutralità tecnologica' può essere considerata lo specchio delle evoluzioni normative sulle comunicazioni elettroniche nel quadro della c.d. convergenza registratesi a partire dal pacchetto di direttive del 2002 sino alle modifiche intercorse tra il 2006 e il 2009[120].

In Italia, ad esempio, l'art. 4 del Codice delle comunicazioni elettroniche, al comma 3, lett. *h*), fissa tra gli obiettivi della disciplina delle reti e dei servizi di comunicazione elettronica quello di garantire la neutralità tecnologica, intesa come la «*non discriminazione tra particolari tecnologie, non imposizione dell'uso di una particolare tecnologia rispetto alle altre e possibilità di adottare provvedimenti ragionevoli al fine di promuovere taluni servizi indipendentemente dalla tecnologia utilizzata*».

---

[118] L'*order* dispone inoltre l'imposizione di uno standard di condotta univoco e chiaro; l'implementazione degli obblighi di trasparenza, attraverso la previsione di un *duty to disclose* posto in capo agli operatori con più abbonati avente per oggetto ogni limitazione di carattere tecnico ed economico che possa in qualche modo compromettere o limitare il servizio offerto. Si impone altresì un formato standard di divulgazione di tali informazioni, che agisce come una sorta di *safe harbor* per i prestatori e, infine si fa salva la possibilità di adottare ragionevoli forme di gestione per fini non commerciali di alcuni tipi di rete (es. reti Wi-Fi senza licenza).

[119] V. FCC, *In the Matter of Protecting and Promoting the Open Internet,* cit. pp. 9, 60 s. e 285: <<§8.11: Any person engaged in the provision of broadcband Internet acess service, insofar as such person is so engaged, shall not unreasonably interfere with or unreasonably disadvantage (i) end users' ability to select, access, and use broadband Internet access service or the lawful Internet content, applications, services, or devices of the choise, or (ii) edge providers' ability to make lawful content, applications, services, or devices available to end users. Reasonable network management shall not be considered a violation of this rule>> v. Aa.Vv., *Riflessioni sull'Open Internet Order della FCC*, cit., p. 2 s.

[120] Cfr. V. Franceschelli, *Convergenza*, Milano, 2009; V.M. Sbrescia, *Le comunicazioni elettroniche tra tecnologia e regolazione*, in *Riv. it. dir. pubbl. comunit.*, 2011, p. 1207 ss.; F. Bassan, *Diritto delle comunicazioni elettroniche*, Milano, 2010

A tale definizione si collegano tre princìpi-cardine quali: *a*) l'accesso, inteso come obbligo di rendere accessibili risorse e servizi ad un'altra impresa al fine di fornire servizi di comunicazione elettronica; *b*) l'interconnessione, ovvero il collegamento fisico e logico tra reti pubbliche di comunicazione, anche tra diversi operatori, al fine di consentire a tutti gli utenti di comunicare tra di loro o di accedere ai servizi offerti da altro operatore e *c*) l'interoperabilità dei servizi, che si concreta nella rimozione di tutti quegli ostacoli regolamentari, tecnici e funzionali che impediscono la fruizione aperta ed interattiva dei servizi di comunicazione[121].

Poste queste premesse, il nuovo Regolamento europeo su neutralità e *roaming* telefonico[122], seppur con maggiore indefinitezza, ricalca le previsioni adottate oltreoceano confermando la necessità di affrontare con un approccio *user-based* il problema della *governance* di Internet.

L'art. 3, n. 1 del Regolamento afferma infatti il diritto per gli utenti di «accedere e distribuire informazioni e contenuti, utilizzare e fornire applicazioni e servizi e utilizzare i dispositivi da loro scelti, a prescindere dalla sede dell'utente finale o del prestatore o dalla localizzazione, dall'origine o dalla destinazione delle informazioni, dei contenuti, delle applicazioni o del servizio».

Il principio procompetitivo di 'ragionevole non interferenza' viene poi frammentato in termini soggettivi: il prestatore di contenuti è libero di offrire servizi qualitativamente migliori, a patto che essi non vadano a discapito della disponibilità o della qualità generale dei servizi di accesso a internet per gli altri utenti (art. 3, n, 4 e 5).

Ai sensi dell'eccezione di cui all'art. 3, n. 3, secondo periodo e ss., il fornitore di accesso è invece autorizzato ad attuare misure ragionevoli di implementazione del traffico nel senso che esse siano trasparenti, non discriminatorie, proporzionate e non si basino su considerazioni di tipo commerciale, ma sull'oggettiva differente qualità tecnica dei requisiti di servizio di specifiche categorie di traffico. Tali misure inoltre non dovranno monitorare lo specifico contenuto né durare più a lungo del necessario[123].

[121] O. Pollicino, *Accesso, interconnessione ed interoperabilità: le novità apportate dal recepimento del "pacchetto telecom" ne confermano il ruolo chiave nel nuovo assetto regolatorio del settore delle comunicazioni elettroniche*, in *Dir. Inf.* 2012, p. 743 ss.

[122] Risoluzione legislativa del Parlamento europeo del 27 ottobre 2015, (10788/2/2015 – C8-0294/2015 – 2013/0309(COD)).

[123] Il Regolamento, in maniera analoga a quanto affermato nelle *bright line rules*, impone inoltre al fornitore di accesso di non bloccare, rallentare, modificare, limitare, interferire con, degradare o discriminare a specifici contenuti, applicazioni o servizi, ad eccezione

Nel rapporto competitivo e osmotico tra i diversi livelli di gestione della rete (infrastruttura, accesso, servizi, raggio d'azione del *prosumer*), un ruolo di equilibrio essenziale è occupato dalla necessità di garantire una tutela flessibile ed articolata dei dati che circolano in un 'mercato' senza confini geografici e di elaborazione, sia in senso protettivo e qualitativo, che ancora in termini concorrenziali (controllo dei trattamenti secondari, portabilità/intercoperabilità[124]) e di tutela dell'utente/consumatore (informazione, trasparenza[125]).

Tali declinazioni del diritto alla privacy [*a*) autodeterminazione informativa; *b*) prodotto di un mercato rilevante a più versanti; *c*) legittima aspettativa del consumatore/utente], convergono verso la nozione di neutralità della rete, intesa come «*diritto che i dati trasmessi e ricevuti in Internet non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuto dei dati, dispositivo utilizzato, applicazioni o, in generale, legittime scelte delle persone*»[126].

L'effettività delle tutele in tema di dati personali rappresenta, pertanto, la precondizione per il pieno esercizio della libertà fondamentale di accedere e svolgere la propria personalità in Internet[127].

---

di quanto necessario e solo per il tempo necessario, al fine di: attuare una norma o un ordine giudiziario comunitario; preservare l'integrità e la sicurezza della rete, dei servizi apprestati e del terminale utente; prevenire la congestione della rete o mitigarne gli effetti.

[124] V. ad es. *Risoluzione Internet aperta*, cit., Considerando 8a: «[…] Le regole contro l'alterazione di contenuti, servizi o applicazioni si riferiscono ad una modifica del contenuto della comunicazione, ma non vietano tecniche di compressione dati non discriminatorie che riducono la dimensione di un file di dati senza alcuna modifica del contenuto. Tale compressione permette un uso più efficiente delle scarse risorse e serve l'interesse degli utenti finali nella riduzione dei volumi di dati, aumentando la velocità e migliorando l'esperienza di utilizzo dei contenuti, servizi o applicazioni in questione».

[125] COM(2015) 192 final, cit., p. 12: «[…] Sebbene l'impatto che esercitano dipenda dal tipo e dal potere di mercato di ciascuna, alcune piattaforme sono in grado di controllare l'accesso ai mercati online e di influire pesantemente sulla remunerazione dei diversi operatori del mercato. Questo stato di cose suscita preoccupazione per il potere sempre maggiore che alcune piattaforme esercitano sul mercato, non da ultimo in termini di opacità sul modo in cui usano le informazioni che acquisiscono, di forte potere contrattuale rispetto a quello dei clienti, che si riflette talvolta nel tenore delle clausole (soprattutto per le PMI), di promozione dei loro propri servizi a scapito dei concorrenti e di politiche di prezzo non trasparenti o limitazioni sui prezzi e le condizioni di vendita».

[126] È la versione dell'art. 4, n. 1 della Dichiarazione dei diritti in Internet redatta dalla Commissione per i diritti e i doveri in Internet istituita in seno alla Camera dei deputati e presieduta dal prof. S. Rodotà, ricalcato per grandi linee dall'art. 3 n. 1 del Regolamento Internet aperto.

[127] B. Croce, *Revisione filosofica dei concetti di «Libertà» e «Giustizia», in La Critica. Rivista di Letteratura, Storia e Filosofia*, 1943, p. 284: «[…] Non c'è cautela che la libertà

Abstract

Moving from the ECJ's decision in the Schrems case, the paper explores the connections between competition, privacy and net neutrality in relation to EU-USA transborder data flows.

Collection, manipulation and accumulation of personal and anonumous information by social media, search engines and other big players in web 2.0, seems to engender a new type of economic surplus that may affect market balance, building and strengthening dominat positions.

In the «big-data»era, stands out the need to promote a data protection in policy more devoted to a «quantitative» approach, trying to ensure the convergence between anti-monopolistic and privacy rules, in the frame of a stronger and more effective enforcement of fundamental rights of solidarity.

non possa e non debba all'occorrenza, usare nel maneggiare le cose dell'economia, che sono rette dalla propria legge alla quale non si comanda *nisi parendo*; ma, del pari, non c'è ardimento che non possa e non debba, in altre occorrenze, osare. Un ardimento tanto più risoluto e sicuro in quanto ubbidisce non a singoli interessi economici di una singola classe sociale, ma unicamente alla voce della coscienza e alla ispirata visione delle vie della storia. […]».

Appendice

1.

Corte di Giustizia dell'Unione Europea

(Grande Sezione)

6 Ottobre 2015
Causa C-362/14

Presidente: Skouris
Relatore: Von Danwitz
Parti: Schrems c. Data Protection Commissioner [Ireland]

1.La domanda di pronuncia pregiudiziale verte sull'interpretazione, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la « Carta »), degli articoli 25, paragrafo 6, e 28 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31), come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003 (GU L 284, pag. 1; in prosieguo: la « direttiva 95/46 »), nonché, in sostanza, sulla validità della decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti » (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti (GU L 215, pag. 7).

2. Tale domanda è stata presentata nell'ambito di una controversia fra il sig. Schrems e il Data Protection Commissioner (commissario per la protezione dei dati; in prosieguo: il « commissario ») concernente il rifiuto, da parte di quest'ultimo, di istruire una denuncia presentata dal sig. Schrems per il fatto che Facebook Ireland Ltd (in prosieguo: « Facebook Ireland ») trasferisce negli Stati Uniti i dati personali dei propri utenti e li conserva su server ubicati in tale paese.

Contesto normativo

La direttiva 95/46
3. I considerando 2, 10, 56, 57, 60, 62 e 63 della direttiva 95/46 così recitano: « (2) […] i sistemi di trattamento dei dati sono al servizio dell'uomo; […] essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire […] al benessere degli individui;

[…]

(10) […] le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[, firmata a Roma il 4 novembre 1950,] e dai principi generali del diritto comunitario; […] pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicu-

rata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità;
[…]
(56) […] lo sviluppo degli scambi internazionali comporta necessariamente il trasferimento oltre frontiera di dati personali; […] la tutela delle persone garantita nella Comunità dalla presente direttiva non osta al trasferimento di dati personali verso paesi terzi che garantiscano un livello di protezione adeguato; […] l'adeguatezza della tutela offerta da un paese terzo deve essere valutata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti;
(57) […] per contro, […] deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato;
[…]
(60) […] comunque i trasferimenti di dati verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione della presente direttiva, in particolare dell'articolo 8;
[…]
(62) […] la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali; (63) […] tali autorità devono disporre dei mezzi necessari all'adempimento dei loro compiti, siano essi poteri investigativi o di intervento, segnatamente in caso di reclami di singoli individui, nonché poteri di avviare azioni legali; […] ».

4. Gli articoli 1, 2, 25, 26, 28 e 31 della direttiva 95/46 dispongono quanto segue:
"Articolo 1"
Oggetto della direttiva
1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali.
[…]
"Articolo 2"
Definizioni
Ai fini della presente direttiva si intende per:
a) "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale;
b) "trattamento di dati personali" ("trattamento"): qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione;
[…]
a. "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari

nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario;

[…]

"Articolo 25"

Principi

1. Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.

2. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.

3. Gli Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2.

4. Qualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione.

5. La Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4.

6. La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona. Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.

"Articolo 26"

Deroghe

1. In deroga all'articolo 25 e fatte salve eventuali disposizioni contrarie della legislazione nazionale per casi specifici, gli Stati membri dispongono che un trasferimento di dati personali verso un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2 può avvenire a condizione che:

a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure

b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure

c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure

d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per co[n]statare, esercitare o difendere un diritto per via

giudiziaria, oppure
e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.
2. Salvo il disposto del paragrafo 1, uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate.
3. Lo Stato membro informa la Commissione e gli altri Stati membri in merito alle autorizzazioni concesse a norma del paragrafo 2.
In caso di opposizione notificata da un altro Stato membro o dalla Commissione, debitamente motivata sotto l'aspetto della tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, la Commissione adotta le misure appropriate secondo la procedura di cui all'articolo
31, paragrafo 2.
Gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione.
[…]

"Articolo 28"
Autorità di controllo

1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.
2. Ciascuno Stato membro dispone che le autorità di controllo siano consultate al momento dell'elaborazione delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.
3. Ogni autorità di controllo dispone in particolare:
— di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;
— di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;
— del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.
È possibile un ricorso giurisdizionale avverso le decisioni dell'autorità di controllo recanti pregiudizio.

4. Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali. La persona interessata viene informata del seguito dato alla sua domanda.
Qualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della presente direttiva. La persona viene ad ogni modo informata che una verifica ha avuto luogo.
[…]
6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro.
[…]
"Articolo 31"
[…]
2. Nei casi in cui è fatto riferimento al presente articolo, si applicano gli articoli 4 e 7 della decisione 1999/468/CE [del Consiglio, del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione (GU L 184, pag. 23)], tenendo conto delle disposizioni dell'articolo 8 della stessa.
[…] ».

La decisione 2000/520

5. La decisione 2000/520 è stata adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46.
6. I considerando 2, 5 e 8 di tale decisione così recitano:
« (2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. In tal caso è possibile trasferire dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.
[…]
(5) Per il trasferimento di dati dalla Comunità agli Stati Uniti, il livello adeguato di protezione di cui alla presente decisione sarebbe raggiunto ove le organizzazioni si conformino ai "principi dell'approdo sicuro in materia di riservatezza" ("The Safe Harbor Privacy Principles"), in prosieguo "i principi", nonché alle "domande più frequenti" ("Frequently Asked Questions"), in prosieguo "FAQ", pubblicate dal governo degli Stati Uniti in data 21 luglio 2000, che forniscono indicazioni per l'attuazione dei principi stessi. Le organizzazioni devono inoltre rendere note pubblicamente le loro politiche in materia di riservatezza e sono sottoposte all'autorità della Commissione federale per il commercio [Federal Trade Commission (FTC)] ai sensi della sezione 5 del Federal Trade Commission Act, che vieta attività o pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, oppure di altri organismi istituiti con legge in grado di assicurare efficacemente il rispetto dei principi applicati in conformità alle FAQ.
[…]
(8) Nell'interesse della trasparenza, e per salvaguardare la facoltà delle competenti autorità degli Stati membri di assicurare la protezione degli individui riguardo al trattamento dei dati personali, è necessario che la presente decisione specifichi le circostanze eccezionali in cui può essere giustificata la sospensione di specifici flussi di dati anche in caso di constatazione di adeguata protezione ».

7. Ai sensi degli articoli da 1 a 4 della decisione 2000/520:
«*Articolo 1*
1. Ai fini dell'applicazione dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, per tutte le attività che rientrano nel campo di applicazione di detta direttiva, si considera che i "Principi di approdo sicuro in materia di riservatezza", in prosieguo i "principi", di cui all'allegato I della presente decisione, applicati in conformità agli orientamenti forniti dalle "Domande più frequenti" (FAQ) di cui all'allegato II della presente decisione, pubblicate dal Dipartimento del commercio degli Stati Uniti in data 21 luglio 2000, garantiscano un livello adeguato di protezione dei dati personali trasferiti dalla Comunità a organizzazioni aventi sede negli Stati Uniti sulla base della seguente documentazione pubblicata dal Dipartimento del commercio degli Stati Uniti:
a) riepilogo delle modalità di esecuzione dei principi di approdo sicuro, di cui all'allegato III;
b) memorandum sui danni per violazioni della riservatezza ed autorizzazioni esplicite previste dalle leggi degli Stati Uniti, di cui all'allegato IV;
c) lettera della Commissione federale per il commercio (FTC), di cui all'allegato V;
d) lettera del Dipartimento dei trasporti degli Stati Uniti, di cui all'allegato VI.
2. Le seguenti condizioni devono sussistere in relazione a ogni singolo trasferimento di dati:
a) l'organizzazione che riceve i dati si è chiaramente e pubblicamente impegnata a conformarsi ai principi applicati in conformità alle FAQ, e
b) detta organizzazione è sottoposta all'autorità prevista per legge di un ente governativo degli Stati Uniti, compreso nell'elenco di cui all'allegato VII, competente ad esaminare denunce e a imporre la cessazione di prassi sleali e fraudolente nonché a disporre il risarcimento di qualunque soggetto, a prescindere dal paese di residenza o dalla nazionalità, danneggiato a seguito del mancato rispetto dei principi applicati in conformità alle FAQ.
3. Le condizioni di cui al paragrafo 2 sono considerate soddisfatte per ogni organizzazione che autocertifica la sua adesione ai principi applicati in conformità alle FAQ a partire dalla data di notifica al Dipartimento del commercio degli Stati Uniti (o all'ente da esso designato) del pubblico annuncio dell'impegno di cui al paragrafo 2, lettera *a*), e dell'identità dell'ente governativo di cui al paragrafo 2, lettera *b*).

"*Articolo 2"*
La presente decisione dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva 95/46/CE. Essa nulla dispone relativamente all'applicazione di altre disposizioni della stessa direttiva, relative al trattamento di dati personali all'interno degli Stati membri e in particolare dell'articolo 4 della stessa.

"*Articolo 3"*
1. Fatto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi applicati in conformità alle FAQ nei casi in cui:
a) gli enti governativi degli Stati Uniti di cui all'allegato VII della presente decisione, o un organismo indipendente di ricorso ai sensi della lettera *a*) del "principio di esecuzione"

di cui all'allegato I della presente decisione abbiano accertato che l'organizzazione viola i principi applicati in conformità alle FAQ, oppure
b) sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare.
La sospensione dei flussi deve cessare non appena sia garantito il rispetto dei principi applicati in conformità alle FAQ e ciò sia stato notificato alle competenti autorità dell'UE.
2. Gli Stati membri comunicano immediatamente alla Commissione
l'adozione di misure a norma del paragrafo 1.
3. Gli Stati membri e la Commissione s'informano altresì a vicenda in merito ai casi in cui l'azione degli organismi responsabili non garantisca la conformità ai principi applicati in conformità alle FAQ negli Stati Uniti.
4. Ove le informazioni di cui ai paragrafi 1, 2 e 3 del presente articolo provino che uno degli organismi incaricati di garantire la conformità ai principi applicati conformemente alle FAQ negli Stati Uniti non svolge la sua funzione in modo efficace, la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure secondo la procedura istituita dall'articolo 31 della direttiva 95/46/CE, al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione.

"Articolo 4"
1. La presente decisione può essere adattata in qualsiasi momento alla luce dell'esperienza acquisita nella sua attuazione e/o qualora il livello di protezione offerta dai principi e dalle FAQ sia superato dai requisiti della legislazione degli Stati Uniti. La Commissione valuta in ogni caso l'applicazione della presente decisione tre anni dopo la sua notifica agli Stati membri sulla base delle informazioni disponibili e comunica qualsiasi riscontro al comitato istituito dall'articolo 31 della direttiva 95/46/CE, fornendo altresì ogni indicazione che possa influire sulla valutazione relativa all'adeguata salvaguardia offerta dalla disposizione di cui all'articolo 1 della presente decisione, ai sensi dell'articolo 25 della direttiva 95/46/CE, nonché di eventuali applicazioni discriminatorie della decisione stessa.
2. La Commissione, se necessario, presenta progetti di opportuni provvedimenti in conformità alla procedura di cui all'articolo 31 della direttiva 95/46/CE ».
8. L'allegato I della decisione 2000/520 così recita:
« Principi di approdo sicuro (safe harbor) del dipartimento del commercio degli Stati Uniti, 21 luglio 2000
[…]
[…] il Dipartimento del commercio sta provvedendo a pubblicare sotto la propria autorità statutaria questo documento e le Frequently Asked Questions ("i principi") al fine di incoraggiare, promuovere e sviluppare il commercio internazionale. I principi sono stati messi a punto in consultazione con l'industria e con il grande pubblico per facilitare gli scambi commerciali fra Stati Uniti ed Unione europea. Essi sono destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta. Giacché questi principi sono stati concepiti esclusivamente a tal fine una loro estensione ad altri fini può non risultare

opportuna. […]
La decisione di un'organizzazione di qualificarsi per l'approdo sicuro è puramente volontaria, e la qualifica può essere ottenuta in vari modi.
[…]
L'adesione a tali principi può essere limitata: *a*) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; *b*) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione; oppure *c*) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata le organizzazioni devono fare il possibile per attuare detti principi integralmente ed in modo trasparente, specificando nelle rispettive politiche in materia di tutela della sfera privata in quali casi saranno regolarmente applicate le eccezioni ammesse dal punto b). Per lo stesso motivo, quando i principi e/o la legislazione statunitense consentono tale scelta, le organizzazioni sono tenute a scegliere, per quanto possibile, la protezione più elevata.
[…] ».
9. L'allegato II della decisione 2000/520 è redatto come segue:
« Domande più frequenti (FAQ)
[…]
FAQ 6 – Autocertificazione
D: Come può un'organizzazione autocertificare la propria adesione ai principi dell'approdo sicuro?
R: Un'organizzazione usufruisce dei vantaggi dell'approdo sicuro dalla data in cui autocertifica al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata l'adesione ai relativi principi, seguendo le indicazioni sotto riportate. Per autocertificare l'adesione all'approdo sicuro un'organizzazione può fornire al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata una lettera, firmata da un proprio funzionario in nome dell'organizzazione che intende aderire all'approdo sicuro, contenente almeno le seguenti informazioni:
1) denominazione dell'organizzazione, indirizzo postale, indirizzo di posta elettronica, numero di telefono e fax;
2) descrizione delle attività dell'organizzazione in rapporto alle informazioni personali pervenute dall'UE;
3) descrizione della politica perseguita dall'organizzazione in merito a dette informazioni personali, che precisi tra l'altro: *a*) dove il pubblico può prenderne conoscenza; *b*) la data della loro effettiva applicazione; *c*) l'ufficio cui rivolgersi per eventuali reclami, richieste di accesso e qualsiasi altra questione riguardante l'approdo sicuro; *d*) lo specifico organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi a possibili pratiche sleali od ingannevoli e a violazioni delle norme legislative e regolamentari che disciplinano la tutela della sfera privata (ed elencati nell'allegato ai principi); *e*) il nome dei programmi concernenti la tutela della sfera privata cui partecipa l'organizzazione; *f*) il metodo di verifica (per esempio all'interno della società, effettuata da terzi) […] e *g*) il meccanismo di ricorso indipendente disponibile per indagare sui reclami non risolti.
Le organizzazioni che intendono estendere i benefici dell'approdo sicuro alle informazioni riguardanti le risorse umane trasferite dall'UE per usi nel contesto di un rapporto di

lavoro possono farlo qualora esista un organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi ad informazioni riguardanti le risorse umane, elencato nell'allegato "Principi di approdo sicuro". […]
Il Dipartimento (o la persona da esso designata) conserverà un elenco di tutte le organizzazioni che inviano queste lettere, assicurando così la disponibilità dei vantaggi legati all'approdo sicuro, ed aggiornerà tale elenco in base alle lettere annuali ed alle notifiche ricevute secondo le modalità precisate nella FAQ 11. […]
[…]
FAQ 11 - Risoluzione delle controversie e modalità di controllo dell'applicazione (enforcement)
D: *Come si applicano le norme derivanti dal principio della garanzia di applicazione (enforcement) per la risoluzione delle controversie, e come si procede se un'organizzazione continua a non rispettare i principi?*
R: Il principio della garanzia di applicazione (enforcement) stabilisce le norme per l'applicazione dell'approdo sicuro. Le modalità di applicazione delle norme di cui al punto b) di tale principio sono illustrate nella domanda sulla verifica (FAQ 7). La presente domanda interessa i punti a) e c), che prescrivono l'istituzione di dispositivi indipendenti di ricorso.
Tali dispositivi possono assumere forme diverse, ma devono soddisfare le prescrizioni formulate nel contesto delle garanzie d'applicazione. Un'organizzazione può adempiere a tali prescrizioni nei modi seguenti: 1) applicando programmi di riservatezza elaborati dal settore privato nei quali siano integrati i principi dell'approdo sicuro e che contemplino dispositivi di attuazione efficaci, del tipo descritto dal principio delle garanzie d'applicazione; 2) uniformandosi a norme giurisdizionali o regolamentari emanate dalle corrispondenti autorità di controllo, che disciplinino il trattamento di reclami individuali e la soluzione delle controversie; oppure 3) impegnandosi a cooperare con le autorità di tutela dei dati aventi sede nella Comunità europea o loro rappresentanti autorizzati.
Quest'elenco è fornito a titolo puramente esemplificativo e non limitativo.
Il settore privato può indicare altri meccanismi di applicazione, purché rispettino il principio delle garanzie d'applicazione e le FAQ. Si noti che le citate garanzie d'applicazione si aggiungono a quelle di cui al paragrafo 3 dell'introduzione ai principi, in forza delle quali le iniziative di autoregolamentazione devono avere carattere vincolante in virtù dell'articolo 5 del Federal Trade Commission Act o analogo testo di legge.
Meccanismi di ricorso:
I consumatori dovrebbero essere incoraggiati a presentare gli eventuali reclami all'organizzazione direttamente interessata, prima di rivolgersi ai dispositivi indipendenti di ricorso. […]
[…]
Attività della Commissione federale per il commercio (Federal Trade Commission, FTC):
La Commissione federale per il commercio (FTC) si è impegnata ad esaminare in via prioritaria i casi trasmessi da organizzazioni di autoregolamentazione in materia di riservatezza (quali BBBOnline e TRUSTe) e dagli Stati membri dell'UE per denunciare la presunta non conformità ai principi dell'approdo sicuro, al fine di stabilire se vi siano state violazioni della sezione 5 del FTC Act, che vieta azioni o pratiche sleali od ingannevoli nel commercio. […]
[…] ».
10. Ai sensi dell'allegato IV della decisione 2000/520:
« Tutela della riservatezza e risarcimento danni, autorizzazioni legali, fusioni e acquisizioni secondo la legge degli Stati Uniti Il presente documento risponde alla richiesta della

Commissione europea di chiarimenti sulla legge statunitense per quanto riguarda *a*) risarcimento dei danni per violazione della sfera privata (privacy), *b*) le "autorizzazioni esplicite" previste dalla legge degli Stati Uniti per l'uso di dati personali in modo contrastante con i principi "approdo sicuro" (safe harbor), *c*) l'effetto delle fusioni e acquisizioni sugli obblighi assunti in base a tali principi.
[…]
B. Autorizzazioni legali esplicite
I principi "approdo sicuro" contengono un'eccezione qualora atti legislativi, regolamenti o la giurisprudenza "comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione".
È ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge. Per quanto riguarda le autorizzazioni esplicite, sebbene i principi "approdo sicuro" intendano colmare le differenze tra il sistema americano e quello europeo relativamente alla tutela della privacy, siamo tenuti al rispetto delle prerogative legislative dei legislatori eletti. La limitata eccezione al rigoroso rispetto dei principi "approdo sicuro" cerca di stabilire un equilibrio in grado di conciliare i legittimi interessi delle parti.
L'eccezione è limitata ai casi in cui esiste un'autorizzazione esplicita.
Tuttavia, come caso limite, la legge, il regolamento o la decisione del tribunale pertinenti devono esplicitamente autorizzare una particolare condotta delle organizzazioni aderenti ai principi "approdo sicuro". In altre parole, l'eccezione non verrà applicata se la legge non prescrive nulla. Inoltre, l'eccezione verrà applicata soltanto se l'esplicita autorizzazione è in conflitto con il rispetto dei principi "approdo sicuro". Anche in questo caso, l'eccezione "si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione".
Ad esempio, se la legge si limita ad autorizzare un'azienda a fornire dati personali alle pubbliche autorità, l'eccezione non verrà applicata. Al contrario, se la legge autorizza espressamente l'azienda a fornire dati personali ad organizzazioni governativ[e] senza il consenso dei singoli, ciò costituisce una "autorizzazione esplicita" ad agire in contrasto con i principi "approdo sicuro". In alternativa, le specifiche eccezioni alle disposizioni relative alla notifica al consenso rientrerebbero nell'ambito dell'eccezione (dato che ciò equivarrebbe ad una specifica autorizzazione a rivelare informazioni senza notifica e consenso). Ad esempio, una legge che autorizzi i medici a fornire le cartelle cliniche dei loro pazienti agli ufficiali sanitari senza il previo consenso dei pazienti stessi potrebbe consentire un'eccezione ai principi di notifica e di scelta.
Tale autorizzazione non permetterebbe ad un medico di fornire le stesse cartelle cliniche alle casse mutue malattie o ai laboratori di ricerca farmaceutica perché ciò esulerebbe dall'ambito degli usi consentiti dalla legge e dunque dall'ambito dell'eccezione […]. L'autorizzazione in questione può essere un'autorizzazione "autonoma" a fare determinate cose con i dati personali ma, come illustrato negli esempi di cui sopra, è probabile che si tratti di un'eccezione a una legge generale che proscrive la raccolta, l'uso o la divulgazione dei dati personali.
[…] ».

La comunicazione COM(2013) 846 final

11. Il 27 novembre 2013 la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio, intitolata « Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA » [COM(2013) 846 final; in prosieguo: la « comunicazione COM(2013) 846 final »]. Tale comunicazione era corredata di una relazione, parimenti datata 27 novembre 2013, contenente le « conclusioni dei copresidenti dell'UE del gruppo di lavoro ad hoc UE-USA sulla protezione dei dati personali » (« Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection »). Tale relazione era stata elaborata, come indicato dal suo punto 1, in cooperazione con gli Stati Uniti d'America in seguito alle rivelazioni dell'esistenza, in tale paese, di diversi programmi di controllo che comprendevano la raccolta e il trattamento su larga scala di dati personali. Detta relazione conteneva, segnatamente, un'analisi dettagliata dell'ordinamento giuridico statunitense per quanto attiene, in particolare, alle basi giuridiche che autorizzano l'esistenza di programmi di controllo, nonché la raccolta e il trattamento di dati personali da parte delle autorità americane.

12. Al punto 1 della comunicazione COM(2013) 846 final, la Commissione ha precisato che «[g]li scambi commerciali sono oggetto della decisione [2000/520]», aggiungendo che tale decisione «fornisce una base giuridica per il trasferimento dei dati personali dall'UE a società stabilite negli Stati Uniti che hanno aderito ai principi d'Approdo sicuro». Inoltre, sempre al punto 1, la Commissione ha messo in evidenza l'importanza sempre maggiore dei flussi di dati personali, legata segnatamente allo sviluppo dell'economia digitale, il quale ha effettivamente «portato a una crescita esponenziale nella quantità, qualità, diversità e natura delle attività di trattamento dei dati».
13. Al punto 2 di tale comunicazione, la Commissione ha osservato che «le preoccupazioni sul livello di protezione dei dati personali dei cittadini dell'[Unione] trasferiti agli Stati Uniti nell'ambito del principio dell'Approdo sicuro sono aumentate», e che «[l]a natura volontaria e dichiarativa del regime ha difatti attirato grande attenzione sulla sua trasparenza
e sulla sua applicazione».

14. Inoltre, essa ha indicato, in questo stesso punto 2, che «[i] dati personali dei cittadini dell'[Unione] inviati negli USA nell'ambito [del] regime [dell'approdo sicuro] possono essere consultati e ulteriormente trattati dalle autorità americane in maniera incompatibile con i motivi per cui erano stati originariamente raccolti nell'[Unione] e con le finalità del loro trasferimento agli Stati Uniti», e che «[l]a maggior parte delle imprese Internet americane che risultano più direttamente interessate [dai] programmi [di controllo], sono certificate nell'ambito del regime Approdo sicuro».

15. Al punto 3.2 della comunicazione COM(2013) 846 final, la Commissione ha rilevato l'esistenza di un certo numero di carenze quanto all'attuazione della decisione 2000/520. Da un lato, essa ha ivi menzionato il fatto che talune imprese americane certificate non rispettavano i principi di cui all'articolo 1, paragrafo 1, della decisione 2000/520 (in prosieguo: i «principi di approdo sicuro») e che dovevano essere apportati miglioramenti a tale decisione concernenti «i punti deboli strutturali relativi alla trasparenza e all'applicazione, i principi sostanziali dell'Approdo sicuro e il funzionamento dell'eccezione per motivi di sicurezza nazionale». Dall'altro, essa ha osservato che l'«Approdo sicuro funge inoltre da interfaccia per il trasferimento di dati personali di cittadini dell'UE dall'[Unione] europea agli Stati Uniti da parte di imprese che sono tenute a consegnare dati ai servizi di intelligence americani nell'ambito dei programmi di raccolta statunitensi».

16. La Commissione ha concluso, a questo stesso punto 3.2, che, se, «[t]enuto conto dei punti deboli individuati, il regime Approdo sicuro non può continuare ad essere applicato secondo le attuali modalità, […] abrogarlo nuocerebbe [tuttavia] agli interessi delle imprese che ne sono membri, nell'[Unione] e negli USA». Infine, sempre a detto punto 3.2, la Commissione ha aggiunto che essa intendeva cominciare «col discutere con le autorità americane i punti deboli individuati».
La comunicazione COM(2013) 847 final

17. Sempre il 27 novembre 2013, la Commissione ha adottato la comunicazione al Parlamento europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite [COM(2013) 847 final; in prosieguo: la «comunicazione COM(2013) 847 final »]. Come risulta dal suo punto 1, tale comunicazione si basava, segnatamente, sulle informazioni ricevute nell'ambito del Gruppo di lavoro ad hoc Unione europea-Stati Uniti e faceva seguito a due relazioni di valutazione della Commissione, pubblicate, rispettivamente, nel 2002 e nel 2004.

18. Il punto 1 di tale comunicazione precisa che il funzionamento della decisione 2000/520 «si basa sugli impegni assunti dalle imprese che vi aderiscono e sulla loro auto-certificazione» e aggiunge che «[l]'adesione è volontaria, ma [che] una volta sottoscritta le norme sono vincolanti».

19. Inoltre, emerge dal punto 2.2 della comunicazione COM(2013) 847 final che, al 26 settembre 2013, 3 246 imprese, facenti parte di numerosi settori dell'economia e dei servizi, erano certificate. Tali imprese fornivano, principalmente, servizi sul mercato interno dell'Unione, in particolare nel settore di Internet, e una parte di esse erano imprese dell'Unione con controllate negli Stati Uniti. Alcune di queste imprese trattavano i dati relativi ai loro dipendenti in Europa e li inviavano in tale paese a fini di gestione delle risorse umane.

20. Sempre al punto 2.2, la Commissione ha sottolineato che «[o]gni insufficienza a livello di trasparenza o di applicazione da parte americana [aveva] l'effetto di far ricadere la responsabilità sulle autorità per la protezione dei dati europee e sulle imprese che si avvalgono del regime in oggetto».

21. Si evince, segnatamente, dai punti da 3 a 5 e 8 della comunicazione COM(2013) 847 final che, nella prassi, un numero considerevole di imprese certificate non rispettava, o rispettava solo in parte, i principi dell'approdo sicuro.

22. Inoltre, al punto 7 di tale comunicazione, la Commissione ha affermato che «tutte le imprese partecipanti al programma PRISM [programma di raccolta di informazioni su larga scala], e che consentono alle autorità americane di avere accesso a dati conservati e trattati negli USA, risultano certificate nel quadro di Approdo sicuro», e che tale sistema « è diventato così una delle piattaforme di accesso delle autorità americane di intelligence alla raccolta di dati personali inizialmente trattati nell'[Unione]». A tal riguardo, la Commissione ha constatato, al punto 7.1 di detta comunicazione, che «un certo numero di basi giuridiche previste dalla legislazione americana consente la raccolta e il trattamento su larga scala di dati personali conservati o altrimenti trattati da società ubicate negli Stati Uniti» e che «[a] causa dell'ampia entità dei programmi, può accadere

che dati trasferiti nell'ambito di Approdo sicuro siano accessibili alle autorità americane e vengano ulteriormente trattati da queste al di là di quanto è necessario e proporzionato alla protezione della sicurezza nazionale come previsto dall'eccezione di cui alla decisione [2000/520]».

23. Al punto 7.2 della comunicazione COM(2013) 847 final, intitolata «Limitazioni e rimedi », la Commissione ha sottolineato che «i principali beneficiari delle garanzie previste dal diritto americano sono i cittadini statunitensi o le persone che risiedono legalmente negli USA» e che «[n]on vi è inoltre alcuna possibilità, né per gli interessati [dell'Unione] che per quelli americani, di ottenere l'accesso, la rettifica o la cancellazione dei dati, o rimedi amministrativi o giurisdizionali in relazione alla raccolta e all'ulteriore trattamento dei loro dati personali nell'ambito dei programmi di controllo statunitensi».

24. Secondo il punto 8 della comunicazione COM(2013) 847 final, fra le imprese certificate figuravano «[l]e imprese del web come Google, Facebook, Microsoft, Apple, Yahoo», le quali contano «[centinaia di] milioni di clienti in Europa» e trasferiscono dati personali negli Stati Uniti a fini del loro trattamento.

25. La Commissione ha concluso, a questo stesso punto 8, che «l'accesso su larga scala, da parte dei servizi di intelligence, ai dati trasferiti negli USA da imprese certificate nell'ambito di Approdo sicuro solleva altri gravi problemi riguardanti la continuità dei diritti dei cittadini europei in materia di protezione in caso di invio dei loro dati negli Stati Uniti».

Procedimento principale e questioni pregiudiziali

26. Il sig. Schrems, cittadino austriaco residente in Austria, è iscritto alla rete sociale Facebook (in prosieguo: «Facebook») dal 2008.

27. Chiunque risieda nel territorio dell'Unione e desideri utilizzare Facebook è tenuto, al momento della sua iscrizione, a sottoscrivere un contratto con Facebook Ireland, una controllata di Facebook Inc., situata, da parte sua, negli Stati Uniti. I dati personali degli utenti di Facebook residenti nel territorio dell'Unione vengono trasferiti, in tutto o in parte, su server di Facebook Inc. ubicati nel territorio degli Stati Uniti, ove essi sono oggetto di un trattamento.

28. Il 25 giugno 2013 il sig. Schrems ha investito il commissario di una denuncia, con la quale lo invitava, in sostanza, ad esercitare le proprie competenze statutarie, vietando a Facebook Ireland di trasferire i suoi dati personali verso gli Stati Uniti. In tale denuncia egli faceva valere che il diritto e la prassi vigenti in tale paese non offrivano una protezione sufficiente dei dati personali conservati nel territorio del medesimo contro le attività di controllo ivi praticate dalle autorità pubbliche. Il sig. Schrems si riferiva, a tal riguardo, alle rivelazioni fatte dal sig. Edward Snowden in merito alle attività dei servizi di intelligence degli Stati Uniti, e in particolare a quelle della National Security Agency (in prosieguo: la «NSA»).

29. Considerando di non essere obbligato a procedere ad un'indagine sui fatti denunciati dal sig. Schrems, il commissario ha respinto la denuncia in quanto priva di fondamento. Egli ha ritenuto, infatti, che non esistessero prove del fatto che la NSA avesse avuto accesso ai dati personali dell'interessato. Il commissario ha aggiunto che le censure formulate

dal sig. Schrems nella sua denuncia non potevano essere fatte valere in maniera utile, in quanto ogni questione relativa all'adeguatezza ella protezione dei dati personali negli Stati Uniti doveva essere risolta in conformità alla decisione 2000/520 e che, in tale decisione, la Commissione aveva constatato che gli Stati Uniti d'America assicuravano un livello di protezione adeguato.

30. Il sig. Schrems ha proposto un ricorso dinanzi alla High Court (Corte d'appello) avverso la decisione di cui al procedimento principale. Dopo aver esaminato le prove prodotte dalle parti nel procedimento principale, tale giudice ha dichiarato che la sorveglianza elettronica e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti rispondevano a finalità necessarie e indispensabili per l'interesse pubblico. Tuttavia, detto giudice ha aggiunto che le rivelazioni del sig. Snowden avevano dimostrato che la NSA ed altri organi federali avevano commesso « eccessi considerevoli ».

31. Orbene, secondo questo stesso giudice, i cittadini dell'Unione non avrebbero alcun diritto effettivo ad essere sentiti. La supervisione sull'operato dei servizi di intelligence verrebbe effettuata nell'ambito di un procedimento segreto e non contraddittorio. Una volta che i dati personali sono stati trasferiti verso gli Stati Uniti, la NSA e altri organi federali, come il Federal Bureau of Investigation (FBI), potrebbero accedere a tali dati nell'ambito della sorveglianza e delle intercettazioni indifferenziate da essi praticate su larga scala. 32. La High Court (Corte d'appello) ha constatato che il diritto irlandese vieta il trasferimento dei dati personali al di fuori del territorio nazionale, fatti salvi i casi in cui il paese terzo in questione assicura un livello di protezione adeguato della vita privata, nonché dei diritti e delle libertà fondamentali. L'importanza dei diritti al rispetto della vita privata e all'inviolabilità del domicilio, garantiti dalla Costituzione irlandese, implicherebbe che qualsiasi ingerenza in tali diritti sia proporzionata e conforme ai requisiti previsti dalla legge.

33. Orbene, l'accesso massiccio e indifferenziato a dati personali sarebbe manifestamente contrario al principio di proporzionalità e ai valori fondamentali protetti dalla Costituzione irlandese. Affinché intercettazioni di comunicazioni elettroniche possano essere considerate conformi a tale Costituzione, occorrerebbe dimostrare che tali intercettazioni sono mirate, che la sorveglianza su talune persone o taluni gruppi di persone è oggettivamente giustificata nell'interesse della sicurezza nazionale o della repressione della criminalità, e che esistono garanzie adeguate e verificabili. Pertanto, secondo la High Court (Corte d'appello), qualora il procedimento principale dovesse essere definito sulla base del solo diritto irlandese, occorrerebbe constatare che, alla luce dell'esistenza di un serio dubbio sul fatto che gli Stati Uniti d'America assicurino un livello di protezione adeguato dei dati personali, il commissario avrebbe dovuto compiere un'indagine sui fatti lamentati dal sig. Schrems nella sua denuncia e che il commissario ha erroneamente respinto quest'ultima.

34. Tuttavia, la High Court (Corte d'appello) considera che tale causa verte sull'attuazione del diritto dell'Unione ai sensi dell'articolo 51 della Carta, cosicché la legittimità della decisione di cui al procedimento principale deve essere valutata sulla scorta del diritto dell'Unione. Orbene, secondo tale giudice, la decisione 2000/520 non soddisfa i requisiti risultanti sia dagli articoli 7 e 8 della Carta sia dai principi enunciati dalla Corte nella sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238). Il diritto al rispetto della vita privata, garantito dall'articolo 7 della Carta e dai valori fondamentali

comuni alle tradizioni degli Stati membri, sarebbe svuotato di significato qualora i pubblici poteri fossero autorizzati ad accedere alle comunicazioni elettroniche su base casuale e generalizzata, senza alcuna giustificazione oggettiva fondata su motivi di sicurezza nazionale o di prevenzione della criminalità, specificamente riguardanti i singoli interessati, e senza che tali pratiche siano accompagnate da garanzie adeguate e verificabili.

35. La High Court (Corte d'appello) osserva, inoltre, che il sig. Schrems, nel suo ricorso, ha contestato in realtà la legittimità del regime dell'approdo sicuro istituito dalla decisione 2000/520 e sul quale poggia la decisione di cui al procedimento principale. Pertanto, anche se il sig. Schrems non ha formalmente contestato la validità né della direttiva 95/46 né della decisione 2000/520, secondo tale giudice occorre chiarire se, avuto riguardo all'articolo 25, paragrafo 6, di tale direttiva, il commissario fosse vincolato dalla constatazione effettuata dalla Commissione in tale decisione, secondo la quale gli Stati Uniti d'America garantiscono un livello di protezione adeguato, oppure se l'articolo 8 della Carta autorizzasse il commissario a discostarsi, se del caso, da una siffatta constatazione.

36. È in tale contesto che la High Court (Corte d'appello) ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali:
«1) Se, nel decidere in merito a una denuncia presentata a un'autorità indipendente investita per legge delle funzioni di gestione e di applicazione della legislazione sulla protezione dei dati, secondo cui i dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti d'America) il cui diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, tenuto conto degli articoli 7, 8 e 47 della Carta, nonostante le disposizioni dell'articolo 25, paragrafo 6, della direttiva 95/46.
2) Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520 ».

Sulle questioni pregiudiziali

37. Con le sue questioni pregiudiziali, che occorre esaminare congiuntamente, il giudice del rinvio chiede, in sostanza, se e in che misura l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, debba essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520, con la quale la Commissione constata che un paese terzo assicura un livello di protezione adeguato, osti a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, possa esaminare la domanda di una persona relativa alla tutela dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, allorché tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non assicurano un livello di protezione adeguato.
Sui poteri delle autorità nazionali di controllo ai sensi dell'articolo 28 della direttiva 95/46, in presenza di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di tale direttiva

38. Occorre rammentare, in via preliminare, che le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà

fondamentali e, segnatamente, al diritto al rispetto della vita privata, devono essere necessariamente interpretate alla luce dei diritti fondamentali garantiti dalla Carta (v. sentenze Österreichischer Rundfunk e a., C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 68; Google Spain e Google, C-131/12, EU:C:2014:317, punto 68, nonché Ryneš, C-212/13, EU:C:2014:2428, punto 29).

39. Risulta dall'articolo 1, nonché dai considerando 2 e 10 della direttiva 95/46, che essa è intesa a garantire non solo una tutela efficace e completa delle libertà e dei diritti fondamentali delle persone fisiche, e segnatamente del diritto fondamentale al rispetto della vita privata con riguardo al trattamento dei dati personali, ma anche un livello elevato di protezione di tali libertà e diritti fondamentali. L'importanza sia del diritto fondamentale al rispetto della vita privata, garantito dall'articolo 7 della Carta, sia del diritto fondamentale alla tutela dei dati personali, garantito dall'articolo 8 della stessa, è inoltre sottolineata nella giurisprudenza della Corte (v. sentenze Rijkeboer, C-553/07, EU:C:2009:293, punto 47; Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 53, nonché Google Spain e Google, C-131/12, EU:C:2014:317, punti 53, 66 e 74 e la giurisprudenza ivi citata).

40. Per quanto attiene ai poteri di cui dispongono le autorità di controllo nazionali quanto al trasferimento di dati personali verso paesi terzi, si deve rilevare che l'articolo 28, paragrafo 1, della direttiva 95/46 obbliga gli Stati membri ad istituire una o più autorità pubbliche incaricate di controllare in piena indipendenza l'osservanza delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento di tali dati. Detto obbligo risulta altresì dal diritto primario dell'Unione, segnatamente dall'articolo 8, paragrafo 3, della Carta e dall'articolo 16, paragrafo 2, TFUE (v., in tal senso, sentenze Commissione/Austria, C-614/10, EU:C:2012:631, punto 36, e Commissione/Ungheria, C-288/12, EU:C:2014:237, punto 47).

41. La garanzia d'indipendenza delle autorità nazionali di controllo è diretta ad assicurare che il controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali sia efficace e affidabile e deve essere interpretata alla luce di tale finalità. Essa è stata disposta al fine di rafforzare la protezione delle persone e degli organismi interessati dalle decisioni di tali autorità. L'istituzione, negli Stati membri, di autorità di controllo indipendenti, costituisce quindi, come rilevato dal considerando 62 della direttiva 95/46, un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali (v. sentenze Commissione/Germania, C-518/07, EU:C:2010:125, punto 25, nonché Commissione/Ungheria C-288/12, EU:C:2014:237, punto 48 e la giurisprudenza ivi citata).

42. Al fine di garantire tale protezione, le autorità nazionali di controllo devono, segnatamente, assicurare un giusto equilibrio fra, da un lato, il rispetto del diritto fondamentale alla vita privata e, dall'altro, gli interessi che impongono una libera circolazione dei dati personali (v., in tal senso, sentenze Commissione/Germania, C-518/07, EU:C:2010:125, punto 24, e Commissione/Ungheria C-288/12, EU:C:2014:237, punto 51).

43. A tal fine, dette autorità dispongono di un'ampia gamma di poteri e questi, elencati in maniera non esaustiva all'articolo 28, paragrafo 3, della direttiva 95/46, costituiscono altrettanti mezzi necessari all'adempimento dei loro compiti, come sottolineato dal considerando 63 di tale direttiva. In tal senso, dette autorità godono, segnatamente, di poteri

investigativi, come quello di raccogliere qualsiasi informazione necessaria all'esercizio della loro funzione di controllo, di poteri effettivi d'intervento, come quello di vietare a titolo provvisorio o definitivo un trattamento di dati o, ancora, del potere di promuovere azioni giudiziarie.

44. È vero che si evince dall'articolo 28, paragrafi 1 e 6, della direttiva 95/46 che i poteri delle autorità nazionali di controllo riguardano i trattamenti di dati personali effettuati nel territorio del loro Stato membro, cosicché esse non dispongono di poteri, sulla base di tale articolo 28, con riguardo ai trattamenti di siffatti dati effettuati nel territorio di un paese terzo.

45. Tuttavia, l'operazione consistente nel far trasferire dati personali da uno Stato membro verso un paese terzo costituisce, di per sé, un trattamento di dati personali ai sensi dell'articolo 2, lettera *b*), della direttiva 95/46 (v., in tal senso, sentenza Parlamento/Consiglio e Commissione, C-317/04 e C-318/04, EU:C:2006:346, punto 56) effettuato nel territorio di uno Stato membro. Infatti, tale disposizione definisce il «trattamento di dati personali» alla stregua di «qualsiasi operazione o insieme di operazioni compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali» e menziona, a titolo di esempio, «la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione».

46. Il considerando 60 della direttiva 95/46 precisa che i trasferimenti di dati personali verso i paesi terzi possono aver luogo soltanto nel pieno rispetto delle disposizioni prese dagli Stati membri in applicazione di tale direttiva. A tal riguardo, il capo IV di detta direttiva, nel quale figurano gli articoli 25 e 26 della medesima, ha predisposto un regime che mira a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i paesi terzi. Tale regime è complementare al regime generale attuato dal capo II di questa stessa direttiva, riguardante le condizioni generali di liceità dei trattamenti di dati personali (v., in tal senso, sentenza Lindqvist, C-101/01, EU:C:2003:596, punto 63).

47. Poiché le autorità nazionali di controllo sono incaricate, ai sensi dell'articolo 8, paragrafo 3, della Carta e dell'articolo 28 della direttiva 95/46, di sorvegliare il rispetto delle norme dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, ciascuna di esse è quindi investita della competenza a verificare se un trasferimento di dati personali dal proprio Stato membro verso un paese terzo rispetti i requisiti fissati dalla direttiva 95/46.

48. Riconoscendo al contempo, al suo considerando 56, che i trasferimenti di dati personali dagli Stati membri verso paesi terzi sono necessari allo sviluppo degli scambi internazionali, la direttiva 95/46 pone come principio, al suo articolo 25, paragrafo 1, che siffatti trasferimenti possano avere luogo soltanto se tali paesi terzi garantiscono un livello di protezione adeguato.

49. Inoltre, il considerando 57 di detta direttiva precisa che i trasferimenti di dati personali verso paesi terzi che non offrono un livello di protezione adeguato devono essere vietati.

50. Al fine di controllare i trasferimenti di dati personali verso i paesi terzi in funzione

del livello di protezione ad essi accordato in ciascuno di tali paesi, l'articolo 25 della direttiva 95/46 impone una serie di obblighi agli Stati membri e alla Commissione. Risulta, segnatamente, da tale articolo, che la constatazione se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuata, come rilevato dall'avvocato generale al paragrafo 86 delle sue conclusioni, vuoi dagli Stati membri vuoi dalla Commissione.

51. La Commissione può adottare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, una decisione che constata che un paese terzo garantisce un livello di protezione adeguato. Conformemente al secondo comma di tale disposizione, una siffatta decisione ha come destinatari gli Stati membri, i quali devono adottare le misure necessarie per conformarvisi. Ai sensi dell'articolo 288, quarto comma, TFUE, essa ha un carattere vincolante per tutti gli Stati membri destinatari e si impone pertanto a tutti i loro organi (v., in tal senso, sentenze Albako Margarinefabrik, 249/85, EU:C:1987:245, punto 17, e Mediaset, C-69/13, EU:C:2014:71, punto 23), nella parte in cui produce l'effetto di autorizzare trasferimenti di dati personali dagli Stati membri verso il paese terzo da essa interessato.

52. Pertanto, fintantoché la decisione della Commissione non sia stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi, fra i quali figurano le loro autorità di controllo indipendenti, non possono certo adottare misure contrarie a tale decisione, come atti intesi a constatare con effetto vincolante che il paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato. Infatti, gli atti delle istituzioni dell'Unione si presumono, in linea di principio, legittimi e producono pertanto effetti giuridici, finché non siano stati revocati o annullati nel contesto di un ricorso per annullamento ovvero dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità (sentenza Commissione/Grecia, C-475/01, EU:C:2004:585, punto 18 e la giurisprudenza ivi citata).

53. Tuttavia, una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, relativa alla protezione dei loro diritti e delle loro libertà con riguardo al trattamento di tali dati. Analogamente, una decisione di tale natura non può, come rilevato dall'avvocato generale, segnatamente, ai paragrafi 61, 93 e 116 delle sue conclusioni, né elidere né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall'articolo 8, paragrafo 3, della Carta, nonché dall'articolo 28 di detta direttiva.

54. Né l'articolo 8, paragrafo 3, della Carta né l'articolo 28 della direttiva 95/46 escludono dall'ambito di competenza delle autorità nazionali di controllo il controllo dei trasferimenti di dati personali verso paesi terzi che sono stati oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, di tale direttiva.

55. In particolare, l'articolo 28, paragrafo 4, primo comma, della direttiva 95/46, il quale dispone che «[q]ualsiasi persona […] può presentare [alle autorità nazionali di controllo] una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali», non prevede alcuna eccezione a tal riguardo nel caso in cui la Commissione abbia adottato una decisione in forza dell'articolo 25, paragrafo 6, di

tale direttiva.

56. Inoltre, sarebbe contrario al sistema predisposto dalla direttiva 95/46, nonché alla finalità degli articoli 25 e 28 della stessa se una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, di detta direttiva avesse come effetto di impedire ad un'autorità nazionale di controllo di esaminare la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali che sono stati o potrebbero essere trasferiti da uno Stato membro verso un paese terzo interessato da tale decisione.

57. Al contrario, l'articolo 28 della direttiva 95/46 si applica, per la sua stessa natura, a ogni trattamento di dati personali. Pertanto, anche in presenza di una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, di tale direttiva, le autorità nazionali di controllo investite da una persona di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei dati personali che la riguardano, devono poter verificare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti fissati da detta direttiva.

58. Se così non fosse, le persone i cui dati personali sono stati o potrebbero essere trasferiti verso il paese terzo di cui trattasi sarebbero private del diritto, garantito all'articolo 8, paragrafi 1 e 3, della Carta, di investire le autorità nazionali di controllo di una domanda ai fini della protezione dei loro diritti fondamentali (v., per analogia, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 68).

59. Una domanda, ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46, con la quale una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo fa valere, come nel procedimento principale, che il diritto e la prassi di tale paese non assicurano, nonostante quanto constatato dalla Commissione in una decisione adottata in base all'articolo 25, paragrafo 6, di tale direttiva, un livello di protezione adeguato, deve essere intesa nel senso che essa verte, in sostanza, sulla compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

60. A tal riguardo, occorre richiamare la giurisprudenza costante della Corte secondo la quale l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali (v., in tal senso, sentenze Commissione e a./Kadi, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66; Inuit Tapiriit Kanatami e a./Parlamento e Consiglio, C-583/11 P, EU:C:2013:625, punto 91, nonché Telefónica/Commissione, C-274/12 P, EU:C:2013:852, punto 56). Le decisioni della Commissione adottate in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 non possono pertanto sfuggire ad un siffatto controllo.

61. Ciò premesso, la Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, quale una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46; la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione (v. sentenze Melki e Abdeli, C-188/10 e C-189/10, EU:C:2010:363, punto 54, nonché CIVAD, C-533/10, EU:C:2012:347, punto 40).

62. Per quanto i giudici nazionali siano effettivamente legittimati ad esaminare la validità di un atto dell'Unione, come una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, essi non sono tuttavia competenti a constatare essi stessi l'invalidità di un siffatto atto (v., in tal senso, sentenze Foto-Frost, 314/85, EU:C:1987:452, punti da 15 a 20, nonché IATA e ELFAA, C-344/04, EU:C:2006:10, punto 27). A fortiori, in sede di esame di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, avente ad oggetto la compatibilità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di detta direttiva con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona,le autorità nazionali di controllo non sono competenti a constatare esse stesse l'invalidità di una siffatta decisione.

63. Alla luce di tali considerazioni, qualora una persona i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo che è stato oggetto di una decisione della Commissione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, investa un'autorità nazionale di controllo di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di tali dati e contesti, in occasione di tale domanda, come nel procedimento principale, la compatibilità di tale decisione con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona, incombe a tale autorità esaminare detta domanda con tutta la diligenza richiesta.

64. Nel caso in cui detta autorità pervenga alla conclusione che gli elementi addotti a sostegno di una siffatta domanda sono privi di fondamento e, per questo motivo, la respinga, la persona che ha proposto detta domanda deve avere accesso, come si evince dall'articolo 28, paragrafo 3, secondo comma, della direttiva 95/46, in combinato con l'articolo 47 della Carta, ai mezzi di ricorso giurisdizionali che le consentono di contestare una siffatta decisione impugnandola dinanzi ai giudici nazionali. Alla luce della giurisprudenza citata ai punti 61 e 62 della presente sentenza, tali giudici devono sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità, allorché essi ritengono che uno o più motivi di invalidità formulati dalle parti o, eventualmente, sollevati d'ufficio siano fondati (v., in tal senso, sentenza T & L Sugars e Sidul Açúcares/Commissione, C-456/13 P, EU:C:2015:284, punto 48 e la giurisprudenza ivi citata).

65. Nell'ipotesi contraria, in cui detta autorità reputi fondate le censure sollevate dalla persona che l'ha investita di una domanda relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento dei suoi dati personali, questa stessa autorità, ai sensi dell'articolo 28, paragrafo 3, primo comma, terzo trattino, della direttiva 95/46, in combinato, segnatamente, con l'articolo 8, paragrafo 3, della Carta, deve poter promuovere azioni giudiziarie. A tal riguardo, incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudici nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione.

66. In virtù delle considerazioni che precedono, si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale

disposizione, quale la decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.

Sulla validità della decisione 2000/520

67. Come si evince dalle spiegazioni del giudice del rinvio relative alle questioni sollevate, il sig. Schrems fa valere, nel procedimento principale, che il diritto e la prassi degli Stati Uniti non assicurano un livello di protezione adeguato ai sensi dell'articolo 25 della direttiva 95/46. Come rilevato dall'avvocato generale ai paragrafi 123 e 124 delle sue conclusioni, il sig. Schrems esprime dubbi, che tale giudice sembra peraltro condividere nella sostanza, concernenti la validità della decisione 2000/520. In tali circostanze, in virtù delle constatazioni effettuate ai punti da 60 a 63 della presente sentenza, e al fine di fornire una risposta completa a detto giudice, occorre verificare se tale decisione sia conforme ai requisiti risultanti da detta direttiva, letta alla luce della Carta.
Sui requisiti risultanti dall'articolo 25, paragrafo 6, della direttiva 95/46

68. Come è già stato rilevato ai punti 48 e 49 della presente sentenza, l'articolo 25, paragrafo 1, della direttiva 95/46 vieta i trasferimenti di dati personali verso un paese terzo che non garantisce un livello di protezione adeguato.

69. Tuttavia, ai fini del controllo di tali trasferimenti, l'articolo 25, paragrafo 6, primo comma, di tale direttiva, dispone che la Commissione «può constatare […] che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 [di tale articolo], in considerazione della sua legislazione nazionale o dei suoi impegni internazionali […], ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

70. È vero che né l'articolo 25, paragrafo 2, della direttiva 95/46 né nessun'altra disposizione della medesima contengono una definizione della nozione di livello di protezione adeguato. In particolare, l'articolo 25, paragrafo 2, di detta direttiva si limita ad enunciare che l'adeguatezza del livello di protezione garantito da un paese terzo «è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati» ed elenca, in maniera non esaustiva, le circostanze che devono essere prese in considerazione in occasione di una siffatta valutazione.

71. Tuttavia, da un lato, come si evince dalla lettera stessa dell'articolo 25, paragrafo 6, della direttiva 95/46, tale disposizione esige che un paese terzo « garantisc[a] » un livello di protezione adeguato in considerazione della sua legislazione nazionale o dei suoi impegni internazionali. Dall'altro, sempre secondo tale disposizione, l'adeguatezza della protezione assicurata dal paese terzo viene valutata «ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona».

72. In tal modo, l'articolo 25, paragrafo 6, della direttiva 95/46 attua l'obbligo esplicito di protezione dei dati personali previsto all'articolo 8, paragrafo 1, della Carta e mira ad

assicurare, come rilevato dall'avvocato generale al paragrafo 139 delle sue conclusioni, la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo.

73. È vero che il termine «adeguato» figurante all'articolo 25, paragrafo 6, della direttiva 95/46 implica che non possa esigersi che un paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, come rilevato dall'avvocato generale al paragrafo 141 delle sue conclusioni, l'espressione «livello di protezione adeguato» deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta. Infatti, in assenza di un siffatto requisito, l'obiettivo menzionato al punto precedente della presente sentenza sarebbe disatteso. Inoltre, il livello elevato di protezione garantito dalla direttiva 95/46, letta alla luce della Carta, potrebbe essere facilmente eluso da trasferimenti di dati personali dall'Unione verso paesi terzi ai fini del loro trattamento in tali paesi.

74. Si evince dalla formulazione espressa dell'articolo 25, paragrafo 6, della direttiva 95/46 che è l'ordinamento giuridico del paese terzo interessato dalla decisione della Commissione che deve garantire un livello di protezione adeguato. Anche se gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, possono essere diversi da quelli attuati all'interno dell'Unione al fine di garantire il rispetto dei requisiti risultanti da tale direttiva, letta alla luce della Carta, tali strumenti devono cionondimeno rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione.

75. In tali condizioni, in sede di esame del livello di protezione offerto da un paese terzo, la Commissione è tenuta a valutare il contenuto delle norme applicabili in tale paese risultanti dalla legislazione nazionale o dagli impegni internazionali di quest'ultimo, nonché la prassi intesa ad assicurare il rispetto di tali norme; al riguardo, tale istituzione deve prendere in considerazione, in conformità all'articolo 25, paragrafo 2, della direttiva 95/46, tutte le circostanze relative ad un trasferimento di dati personali verso un paese terzo.

76. Analogamente, alla luce del fatto che il livello di protezione assicurato da un paese terzo può evolversi, incombe alla Commissione, successivamente all'adozione di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, verificare periodicamente se la constatazione relativa al livello di protezione adeguato assicurato dal paese terzo in questione continui ad essere giustificata in fatto e in diritto. Una siffatta verifica è in ogni caso obbligatoria quando taluni indizi facciano sorgere un dubbio al riguardo.

77. Inoltre, come rilevato dall'avvocato generale ai paragrafi 134 e 135 delle sue conclusioni, in sede di esame della validità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, della direttiva 95/46, occorre anche tenere conto delle circostanze intervenute successivamente all'adozione di tale decisione.

78. A tal riguardo, occorre constatare che, alla luce, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al

rispetto della vita privata e, dall'altro, del numero significativo di persone i cui diritti fondamentali possono essere violati in caso di trasferimento di dati personali verso un paese terzo che non assicura un livello di protezione adeguato, il potere discrezionale della Commissione in ordine all'adeguatezza del livello di protezione assicurato da un paese terzo risulta ridotto, cosicché è necessario procedere ad un controllo stretto dei requisiti risultanti dall'articolo 25 della direttiva 95/46, letto alla luce della Carta (v., per analogia, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 47 e 48).

Sull'articolo 1 della decisione 2000/520

79. La Commissione ha considerato, all'articolo 1, paragrafo 1, della decisione 2000/520, che i principi di cui all'allegato I della medesima, applicati in conformità agli orientamenti forniti dalle FAQ di cui all'allegato II di detta decisione, garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'Unione a organizzazioni aventi sede negli Stati Uniti. Risulta da tale disposizione che sia tali principi sia tali FAQ sono stati pubblicati dal Dipartimento del commercio degli Stati Uniti.

80. L'adesione di un'organizzazione ai principi dell'approdo sicuro avviene sulla base di un sistema di autocertificazione, come si evince dall'articolo 1, paragrafi 2 e 3, di tale decisione, in combinato disposto con la FAQ 6 figurante all'allegato II a detta decisione.

81. Sebbene il ricorso, da parte di un paese terzo, ad un sistema di autocertificazione non sia di per sé contrario al requisito previsto dall'articolo 25, paragrafo 6, della direttiva 95/46, secondo il quale il paese terzo di cui trattasi deve garantire un livello di protezione adeguato «in considerazione della […] legislazione nazionale o [degli] impegni internazionali» di tale paese, l'affidabilità di un siffatto sistema, con riferimento a tale requisito, poggia essenzialmente sulla predisposizione di meccanismi efficaci di accertamento e di controllo che consentano di individuare e sanzionare, nella prassi, eventuali violazioni delle norme che assicurano la protezione dei diritti fondamentali, e segnatamente del diritto al rispetto della vita privata, nonché del diritto alla protezione dei dati personali.

82. Nella specie, in forza dell'allegato I, secondo comma, della decisione 2000/520, i principi dell'approdo sicuro sono «destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta». Tali principi sono dunque applicabili soltanto alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti principi.

83. Inoltre, ai sensi dell'articolo 2 della decisione 2000/520, quest'ultima «dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi [dell'approdo sicuro] applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva [95/46]», senza tuttavia contenere le constatazioni sufficienti quanto alle misure tramite le quali gli Stati Uniti d'America assicurano un livello di protezione adeguato, ai sensi dell'articolo 25, paragrafo 6, di tale direttiva, in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

84. A ciò si aggiunge che, in conformità all'allegato I, quarto comma, della decisione

2000/520, l'applicabilità di detti principi può essere limitata, segnatamente, «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]», nonché da «disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione».

85. A tal riguardo, al titolo B del suo allegato IV, la decisione 2000/520 sottolinea, per quanto attiene ai limiti ai quali è assoggettata l'applicabilità dei principi dell'approdo sicuro, che «[è] ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge».

86. In tal modo, la decisione 2000/520 sancisce il primato delle «esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]» sui principi dell'approdo sicuro, primato in forza del quale le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime.

87. Alla luce del carattere generale della deroga figurante all'allegato I, quarto comma, della decisione 2000/520, essa rende pertanto possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti. A tal riguardo, poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 33 e la giurisprudenza ivi citata).

88. Inoltre, la decisione 2000/520 non contiene alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti, ingerenze che entità statali di tale paese sarebbero autorizzate a compiere laddove perseguano obiettivi legittimi, come la sicurezza nazionale.

89. A ciò si aggiunge il fatto che la decisione 2000/520 non menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura. Come rilevato dall'avvocato generale ai paragrafi da 204 a 206 delle sue conclusioni, i meccanismi di arbitrato privato e i procedimenti dinanzi alla Commissione federale per il commercio, i cui poteri, descritti segnatamente nelle FAQ 11 figuranti all'allegato II a tale decisione, sono limitati alle controversie in materia commerciale, riguardano il rispetto, da parte delle imprese americane, dei principi dell'approdo sicuro, e non possono essere applicati nell'ambito delle controversie concernenti la legittimità di ingerenze nei diritti fondamentali risultanti da misure di origine statale.

90. Inoltre, la suesposta analisi della decisione 2000/520 è corroborata dalla valutazione della stessa Commissione quanto alla situazione risultante dall'esecuzione di tale decisione. Infatti, in particolare ai punti 2 e 3.2 della comunicazione COM(2013) 846 final, nonché ai punti 7.1, 7.2 e 8 della comunicazione COM(2013) 847 final, il cui contenuto viene illustrato rispettivamente ai punti da 13 a 16, nonché ai punti 22, 23 e 25 della presente sentenza, tale istituzione ha constatato che le autorità americane potevano accedere ai dati personali trasferiti dagli Stati membri verso gli Stati Uniti e trattarli in maniera incompatibile, segnatamente, con le finalità del loro trasferimento, e al di là di quanto era strettamente necessario e proporzionato per la protezione della sicurezza nazionale. Analogamente, la Commissione ha constatato che non esistevano, per le persone di cui trattasi, rimedi amministrativi o giurisdizionali che consentissero, segnatamente, di accedere ai dati che le riguardavano e, se del caso, di ottenerne la rettifica o la soppressione.

91. Quanto al livello di protezione delle libertà e dei diritti fondamentali garantito all'interno dell'Unione, una normativa della medesima che comporta un'ingerenza nei diritti fondamentali garantiti dagli articoli 7 e 8 della Carta deve prevedere, secondo la giurisprudenza costante della Corte, regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati personali sono interessati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti 54 e 55, nonché la giurisprudenza ivi citata).

92. Inoltre, e soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario (sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 52 e la giurisprudenza ivi citata).

93. In tal senso, non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta [v. in tal senso, in relazione alla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, (GU L 105, pag. 54), sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punti da 57 a 61].

94. In particolare, si deve ritenere che una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta (v., in tal senso, sentenza Digital Rights Ireland e a., C-293/12 e C-594/12, EU:C:2014:238, punto 39).

95. Analogamente, una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta. Infatti, l'articolo 47, primo comma, della Carta esige che ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati abbia diritto ad un ricorso effettivo dinanzi ad un giudice, nel rispetto delle condizioni previste in tale articolo. A tal riguardo, l'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto (v., in tal senso, sentenze Les Verts/Parlamento, 294/83, EU:C:1986:166, punto 23; Johnston, 222/84, EU:C:1986:206, punti 18 e 19; Heylens e a., 222/86, EU:C:1987:442, punto 14, nonché, UGT-Rioja e a., da C-428/06 a C-434/06, EU:C:2008:488, punto 80).

96. Come è stato rilevato segnatamente ai punti 71, 73 e 74 della presente sentenza, l'adozione, da parte della Commissione, di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione, come emerge segnatamente dai punti precedenti della presente sentenza.

97. Orbene, occorre rilevare che la Commissione, nella decisione 2000/520, non ha affermato che gli Stati Uniti d'America «garantiscono» effettivamente un livello di protezione adeguato in considerazione della loro legislazione nazionale o dei loro impegni internazionali.

98. Di conseguenza, e senza che occorra esaminare i principi dell'approdo sicuro sotto il profilo del loro contenuto, si deve concludere che l'articolo 1 di tale decisione viola i requisiti fissati all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che esso è, per
tale motivo, invalido.

Sull'articolo 3 della decisione 2000/520

99. Si evince dalle considerazioni svolte ai punti 53, 57 e 63 della presente sentenza che, considerato l'articolo 28 della direttiva 95/46, letto alla luce, segnatamente, dell'articolo 8 della Carta, le autorità nazionali di controllo devono poter esaminare, in piena indipendenza, ogni domanda relativa alla protezione dei diritti e delle libertà di una persona con riguardo al trattamento di dati personali che la riguardano. Ciò vale in particolare allorché, in occasione di una siffatta domanda, tale persona sollevi questioni attinenti alla compatibilità di una decisione della Commissione adottata in forza dell'articolo 25, paragrafo 6, di tale direttiva, con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

100. Tuttavia, l'articolo 3, paragrafo 1, primo comma, della decisione 2000/520 con-

tiene una disciplina specifica quanto ai poteri di cui dispongono le autorità nazionali di controllo con riferimento ad una constatazione effettuata dalla Commissione in relazione al livello di protezione adeguato, ai sensi dell'articolo 25 della direttiva 95/46.

101. Così, ai sensi di tale disposizione, tali autorità possono, «[f]atto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva [95/46], […] sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi [della decisione 2000/520]», a condizioni restrittive che fissano una soglia elevata di intervento. Per quanto tale disposizione non pregiudichi i poteri di dette autorità di adottare misure intese ad assicurare il rispetto delle disposizioni nazionali adottate in applicazione di questa direttiva, ciononostante essa esclude che le medesime possano adottare misure intese a garantire il rispetto dell'articolo 25 della direttiva medesima.

102. L'articolo 3, paragrafo 1, primo comma, della decisione 2000/520 deve pertanto essere inteso nel senso che esso priva le autorità nazionali di controllo dei poteri che esse traggono dall'articolo 28 della direttiva 95/46, nel caso in cui una persona, in occasione di una domanda basata su tale disposizione, adduca elementi idonei a rimettere in discussione il fatto che una decisione della Commissione che ha constatato, sul fondamento dell'articolo 25, paragrafo 6, di tale direttiva, che un paese terzo garantisce un livello di protezione adeguato, sia compatibile con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona.

103. Orbene, il potere di esecuzione che il legislatore dell'Unione ha attribuito alla Commissione con l'articolo 25, paragrafo 6, della direttiva 95/46 non conferisce a tale istituzione la competenza di limitare i poteri delle autorità nazionali di controllo previsti al punto precedente della presente sentenza.

104. Ciò premesso, occorre constatare che, adottando l'articolo 3 della decisione 2000/520, la Commissione ha ecceduto la competenza attribuitale all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che, per questo motivo, esso è invalido.

105. Poiché gli articoli 1 e 3 della decisione 2000/520 non possono essere separati dagli articoli 2 e 4, nonché dagli allegati alla medesima, la loro invalidità inficia la validità di tale decisione nel suo complesso.

106. Alla luce di tutte le considerazioni che precedono, si deve concludere che la decisione 2000/520 è invalida.

Sulle spese

107. Nei confronti delle parti nel procedimento principale, la presente causa costituisce un incidente sollevato dinanzi al giudice nazionale, cui spetta quindi statuire sulle spese. Le spese sostenute da altri soggetti per presentare osservazioni alla Corte non possono dar luogo a rifusione.

P.Q.M. — lla Corte (Grande Sezione) dichiara:
1) L'articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del

Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.
2) La decisione 2000/520 è invalida.

2.

Corte di Giustizia dell'Unione Europea

Conclusioni dell'Avvovato generale Yves Bot

Presentate il 23 Settembre 2015

Causa C-362/14
Parti: Schrems
Data Protection Comissioner [Ireland]

1 - Introduzione[1]

1. Come constatato dalla Commissione europea nella sua comunicazione del 27 novembre 2013[2], «[i] trasferimenti di dati personali sono un importante e necessario elemento delle relazioni transatlantiche. Fanno parte integrante degli scambi commerciali fra le due sponde dell'Oceano, anche per i nuovi settori emergenti del digitale come i media sociali o il cloud computing, che vedono grosse quantità di dati viaggiare dall'Unione europea agli Stati Uniti[3]».

2. Gli scambi commerciali sono oggetto della decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative « Domande più frequenti » (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti[4]. Tale decisione fornisce una base giuridica per il trasferimento di dati personali dall'Unione a società stabilite negli Stati Uniti che hanno aderito ai principi di approdo sicuro.

3. Detta decisione deve oggi fare fronte alla sfida di consentire i flussi di dati fra l'Unione e gli Stati Uniti, garantendo al contempo un elevato livello di protezione a tali dati, come richiesto dal diritto dell'Unione.

4. Infatti, recentemente, da alcune rivelazioni è emersa l'esistenza di programmi statunitensi di raccolta di informazioni su larga scala. Tali rivelazioni hanno gettato un'ombra sul rispetto delle norme del diritto dell'Unione in occasione dei trasferimenti di dati personali verso imprese stabilite negli Stati Uniti e hanno evidenziato i limiti del regime dell'approdo sicuro.

5. Il presente rinvio pregiudiziale invita la Corte a precisare l'atteggiamento che le autorità nazionali di controllo e la Commissione devono tenere allorché si trovano di fronte a disfunzioni nell'applicazione della decisione 2000/520.

---

[1] Lingua originale: il francese.
[2] Comunicazione della Commissione al Parlamento europeo e al Consiglio intitolata «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» [COM(2013) 846 def.].
[3] Pagina 2
[4] GU L 215, pag. 7, e rettifica in GU 2001, L 115, pag. 14.

6. La direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[5], prevede, al suo capo IV, norme relative al trasferimento di dati personali verso paesi terzi.

7. All'interno di tale capo, il principio sancito dall'articolo 25, paragrafo 1, di tale direttiva, stabilisce che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati ad essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato a tali dati.

8. Per converso, come indicato dal legislatore dell'Unione al considerando 57 di detta direttiva, deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato.

9. Ai sensi dell'articolo 25, paragrafo 2, della direttiva 95/46, «[l']adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate».

10. Ai sensi dell'articolo 25, paragrafo 6, di tale direttiva, la Commissione può constatare che un paese terzo garantisce, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione adeguato ai dati personali. Non appena la Commissione adotta una decisione in tal senso, il trasferimento di dati personali verso il paese terzo di cui trattasi può avere luogo.

11. In applicazione di detta disposizione, la Commissione ha adottato la decisione 2000/520. Risulta dall'articolo 1, paragrafo 1, di tale decisione, che si considera che i «[p]rincipi di approdo sicuro in materia di riservatezza», applicati in conformità agli orientamenti forniti dalle «Domande più frequenti[6]», garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'Unione a organizzazioni aventi sede negli Stati Uniti.

12. Di conseguenza, la decisione 2000/520 autorizza il trasferimento di dati personali dagli Stati membri verso imprese stabilite negli Stati Uniti che si sono impegnate a rispettare i principi dell'approdo sicuro.

13. La decisione 2000/520 enuncia, al suo allegato I, un certo numero di principi ai quali le imprese possono aderire volontariamente, corredati da limiti e da un sistema di controllo specifico. Il numero di imprese che hanno aderito a quello che potrebbe essere qualificato come un «codice di condotta» era superiore a 3 200 nel 2013.

[5] GU L 281, pag. 31. Direttiva come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio del 29 settembre 2003 (GU L 284, pag. 1; in prosieguo: la « direttiva 95/46 »).

[6] Frequently asked questions; in prosieguo: le «FAQ».

14. Il regime dell'approdo sicuro poggia su una soluzione che mescola l'autocertificazione, nonché l'autovalutazione da parte delle imprese private, e l'intervento dei poteri pubblici.

15. I principi dell'approdo sicuro sono stati messi a punto «in consultazione con l'industria e con il grande pubblico per facilitare gli scambi commerciali fra Stati Uniti ed Unione […]. Essi sono destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione […], al fine di permettere a tali organizzazioni di ottemperare al principio di "approdo sicuro" ed alla presunzione di "adeguatezza" che esso comporta[7]».

16. I principi dell'approdo sicuro, figuranti all'allegato I della decisione 2000/520, prevedono, segnatamente:
— un obbligo di informazione in forza del quale «[l]e organizzazioni devono informare i singoli individui in merito alle finalità per cui vengono raccolte e utilizzate le informazioni su di essi, alle modalità per contattare le organizzazioni in relazione ad eventuali quesiti o reclami, alla tipologia dei terzi a cui vengono fornite le informazioni, e infine ad opzioni e mezzi che le organizzazioni mettono a disposizione dei singoli individui per limitare l'utilizzazione e la rivelazione delle informazioni. Queste indicazioni vanno formulate […] quando si tratti del primo invito a fornire informazioni personali alle organizzazioni rivolto ad una persona oppure non appena ciò risulti successivamente possibile, ma comunque prima che le organizzazioni utilizzino o rivelino per la prima volta a terzi tali informazioni per finalità diverse da quelle per le quali le informazioni stesse erano state originariamente raccolte[8]»;
— un obbligo per le organizzazioni di offrire agli individui la possibilità di scegliere se le informazioni personali che li riguardano vadano rivelate a terzi ovvero utilizzate per fini incompatibili con quelli per cui le informazioni stesse erano state originariamente raccolte o con quelli successivamente autorizzati dall'interessato. Nel caso di dati di carattere delicato, « va data la possibilità di scelta affermativa o esplicita (facoltà di consenso) per quanto riguarda la possibilità che le informazioni in questione vengano rivelate a terzi od utilizzate per scopi diversi da quelli per cui esse erano state originariamente raccolte o da quelli successivamente autorizzati dagli interessati con l'esercizio della facoltà di consenso[9]»;
— norme relative al trasferimento successivo dei dati. In tal senso, «[l]e organizzazioni che comunicano informazioni a terzi devono applicare i principi di notifica e di scelta[10]»;
— quanto alla sicurezza dei dati, un obbligo per «[l]e organizzazioni che detengono, aggiornano, utilizzano o diffondono informazioni personali […] [di] prendere ragionevoli recauzioni per proteggerle da perdita ed abusi nonché da accesso, rivelazione, alterazione e distruzione non autorizzati[11] »;
— quanto all'integrità dei dati, un obbligo per le organizzazioni «[di] prendere provvedimenti ragionevoli per garantire che i dati siano attendibili in funzione dell'uso che si prevede di farne, accurati, completi e aggiornati[12]»;
— che gli individui i cui dati sono in possesso di un'organizzazione devono, in linea di principio, « poter accedere alle informazioni personali che li riguardano […] ed altresì

[7] Secondo comma dell'allegato I della decisione 2000/520.
[8] V. allegato I, *sub* «Notifica».
[9] V. allegato I, *sub* «Scelta»
[10] V. allegato I, *sub* «Trasferimento successivo».
[11] V. allegato I, *sub* «Sicurezza».
[12] V. allegato I, *sub* «Integrità dei dati».

poterle correggere, emendare o cancellare se ed in quanto esse risultino inesatte[13]»;
— un obbligo di prevedere « meccanismi volti a garantire il rispetto dei principi [dell'approdo sicuro], la possibilità di ricorso per gli individui cui si riferiscono i dati che vedano lesi i propri interessi dal mancato rispetto dei principi stessi, e la non impunità di un'organizzazione che non rispetti i principi[14]».

17. Un'organizzazione americana che desideri aderire ai principi dell'approdo sicuro è tenuta a dichiarare, nella sua politica di tutela della sfera privata, di rendere pubblico il fatto di aderire a tali principi e di conformarvisi effettivamente e ad autocertificare, con dichiarazione al Dipartimento del commercio degli Stati Uniti, di essere rispettosa dei medesimi principi[15].

18. Le organizzazioni dispongono di più strumenti per conformarsi ai principi dell'approdo sicuro. Così esse possono, ad esempio, «aderi[re] ad un programma di tutela della riservatezza, messo a punto dal settore privato e tale da ottemperare ai principi in questione [oppure] qualificarsi per l'approdo sicuro sviluppa[ndo] proprie politiche in fatto di riservatezza dei dati personali, purché queste siano conformi ai principi indicati […]. Inoltre, anche le organizzazioni soggette a disposizioni (o a norme) legislative, regolamentari, amministrative o d'altro tipo che tutelino efficacemente la riservatezza dei dati personali possono compiere quanto necessario per godere dei vantaggi dell'approdo sicuro[16]».

19. Esistono diversi meccanismi, i quali mescolano l'arbitrato privato e il controllo ad opera dei poteri pubblici, per verificare il rispetto dei principi dell'approdo sicuro. Il controllo può in tal senso essere assicurato tramite un sistema di risoluzione extragiudiziale delle controversie da parte di un terzo indipendente. Inoltre, le imprese possono impegnarsi a cooperare con il panel dell'Unione sulla protezione dei dati. Infine, la Commissione federale del commercio (Federal Trade Commission; in prosieguo: la «FTC»), sulla base dei poteri conferitile in forza della sezione 5 della legge sulla Commissione federale del commercio (Federal Trade Commission Act), nonché il ministero dei Trasporti (Department of Transportation), sulla base dei poteri che gli sono stati conferiti in virtù dell'articolo 41712 del Codice degli Stati Uniti (United States Code) figurante al suo titolo 49, sono competenti ad esaminare le denunce.

20. Ai sensi del quarto comma dell'allegato I della decisione 2000/520, l'adesione ai principi dell'approdo sicuro può essere limitata, segnatamente, «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia» e «da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione[17]».

21. Inoltre, la possibilità, per le autorità competenti degli Stati membri, di sospendere

[13] V. allegato I, *sub* «Accesso».
[14] V. allegato I, *sub* «Garanzie d'applicazione».
[15] Articolo 1, paragrafi 2 e 3, della decisione 2000/520. V., parimenti, allegato II, FAQ 6.
[16] Terzo comma dell'allegato I.
[17] V., parimenti, allegato IV, B.

flussi di dati è subordinata a diverse condizioni, le quali sono previste all'articolo 3, paragrafo 1, della decisione 2000/520.

22. La presente domanda di pronuncia pregiudiziale induce a porsi interrogativi sulla portata della decisione 2000/520, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (in prosieguo: la « Carta »), nonché degli articoli 25, paragrafo 6, e 28 della direttiva 95/46. Tale domanda è stata presentata nell'ambito di una controversia fra il sig. Schrems e il Data Protection Commissioner (Commissario per la protezione dei dati; in prosieguo: il «commissario») concernente il rifiuto, da parte di quest'ultimo, di istruire una denuncia presentata dal sig. Schrems per il fatto che la Facebook Ireland Ltd (in prosieguo: «Facebook Ireland») conserva i dati personali dei propri iscritti su server ubicati negli Stati Uniti.

23. Il sig. Schrems è un cittadino austriaco residente in Austria. Egli è iscritto al media sociale Facebook dal 2008.

24. A tutti gli utenti di Facebook residenti nel territorio dell'Unione viene chiesto di sottoscrivere un contratto con Facebook Ireland, la quale è una controllata della società madre Facebook Inc., stabilita negli Stati Uniti (in prosieguo: «Facebook USA»). I dati degli iscritti a Facebook Ireland residenti nel territorio dell'Unione vengono, in tutto o in parte, trasferiti e archiviati in server di Facebook USA ubicati nel territorio degli Stati Uniti.

25. Il 25 giugno 2013 il sig. Schrems ha depositato una denuncia dinanzi al commissario, facendo valere, in sostanza, che il diritto e la prassi statunitensi non offrono alcuna protezione effettiva dei dati conservati negli Stati Uniti contro la sorveglianza dello Stato. Ciò emergerebbe dalle rivelazioni fatte dal sig. Snowden a partire dal maggio 2013 in merito alle attività dei servizi di intelligence americani, e in particolare alle attività della National Security Agency (in prosieguo: la «NSA»).

26. Emerge, segnatamente, da tali rivelazioni, che la NSA avrebbe creato un programma chiamato « PRISM », nell'ambito del quale tale agenzia avrebbe ottenuto libero accesso ai dati conservati in massa su server ubicati negli Stati Uniti, posseduti o controllati da una serie di società operanti nel settore di Internet e della tecnologia come Facebook USA.

27. Il commissario ha ritenuto di non essere obbligato ad istruire la denuncia, in quanto essa era priva di fondamento giuridico. Tale autorità ha considerato che non esistevano prove del fatto che la NSA avesse avuto accesso ai dati del sig. Schrems. Inoltre, a suo avviso, la denuncia doveva essere respinta a causa della decisione 2000/520, con la quale la Commissione ha constatato che gli Stati Uniti assicurano, nell'ambito del regime dell'approdo sicuro, un livello adeguato di protezione ai dati personali trasferiti. Ogni questione concernente il carattere adeguato della protezione di tali dati negli Stati Uniti dovrebbe essere risolta in conformità a detta decisione, la quale gli impedirebbe di esaminare il problema sollevato dalla denuncia.

28. La normativa nazionale che ha indotto il commissario a respingere la denuncia è la seguente.

29. L'articolo 10, paragrafo 1, della legge del 1988 sulla protezione dei dati (Data Protection Act 1988), come modificata dalla legge del 2003 sulla protezione dei dati [Data

Protection (Amendment) Act 2003; in prosieguo: la «legge sulla protezione dei dati»] gli conferisce il potere di esaminare le denunce e così recita:
a) commissario può verificare o far verificare se disposizioni della presente legge siano state, siano o rischino di essere violate nei confronti di una determinata persona, o quando tale persona presenta al medesimo una denuncia per una violazione di una qualsiasi di tali disposizioni, o quando il commissario ritenga che una siffatta violazione possa esistere.
b) qualora una persona presenti una denuncia dinanzi al commissario in forza della lettera *a*) del presente paragrafo, il commissario:
i) istruisce o fa istruire la denuncia, a meno che non concluda che essa sia defatigatoria o vessatoria, e
ii) qualora egli o ella non sia in grado, entro un termine ragionevole, di ottenere dalle parti interessate una risoluzione extragiudiziale dell'oggetto della denuncia, lo stesso notifica per iscritto al denunciante la decisione adottata in ordine alla medesima, indicando che, qualora tale decisione gli arrechi pregiudizio, il denunciante può impugnarla in forza dell'articolo 26 della presente legge, entro 21 giorni a partire dal ricevimento della notifica».

30. Nella specie, il commissario ha concluso che la denuncia del sig. Schrems era «defatigatoria o vessatoria», nel senso che essa era destinata al fallimento, in quanto priva di fondamento giuridico. È su tale base che esso si è rifiutato di istruire tale denuncia.

31. L'articolo 11 della legge sulla protezione dei dati disciplina il trasferimento dei dati personali al di fuori del territorio nazionale. L'articolo 11, paragrafo 2, lettera *a*), della medesima prevede quanto segue:

«Qualora, in un procedimento disciplinato dalla presente legge, venga sollevata una questione:
i) per determinare se il livello di protezione adeguato specificato al paragrafo 1 del presente articolo sia assicurato da un paese o da un territorio al di fuori dello Spazio economico europeo [(SEE)] verso il quale vengono trasferiti dati personali, e
ii) sia stata effettuata una constatazione da parte dell'Unione per quanto attiene al tipo di trasferimenti in questione, la questione verrà esaminata in conformità a tale constatazione».

32. L'articolo 11, paragrafo 2, lettera *b*), della legge sulla protezione dei dati, definisce la nozione di constatazione dell'Unione nei seguenti termini:
«Alla lettera *a*) del presente paragrafo, per "constatazione dell'Unione" si intende una constatazione che la Commissione […] ha fatto ai sensi del paragrafo 4 o del paragrafo 6 dell'articolo 25 della direttiva [95/46], nell'ambito del procedimento previsto all'articolo 31, paragrafo 2, della [medesima] al fine di determinare se il livello di protezione adeguato specificato al paragrafo 1 del presente articolo sia assicurato da un paese o un territorio al di fuori del [SEE].»

33. Il commissario ha osservato che la decisione 2000/520 era una «constatazione dell'Unione» ai sensi dell'articolo 11, paragrafo 2, lettera *a*), della legge sulla protezione dei dati, cosicché, in forza di tale legge, ogni questione relativa all'adeguatezza della protezione dei dati personali nel paese terzo in cui essi vengono trasferiti doveva essere esaminata in conformità a tale constatazione. Dal momento che in ciò consisteva essenzialmente la denuncia del sig. Schrems, vale a dire il trasferimento di dati personali in un paese terzo che,

in pratica, non assicurava un livello di protezione adeguato, il commissario ha ritenuto che la natura e l'esistenza stessa della decisione 2000/520 gli impedissero di esaminare tale questione.

34. Il sig. Schrems ha presentato un ricorso dinanzi alla Corte d'appello avverso la decisione del commissario di respingere la sua denuncia. Dopo aver esaminato le prove prodotte nel procedimento principale, tale giudice ha constatato che la sorveglianza elettronica e l'intercettazione dei dati personali rispondono a finalità necessarie e indispensabili per l'interesse pubblico, ossia il mantenimento della sicurezza nazionale e la prevenzione dei crimini gravi. La Corte d'appello indica, a tal riguardo, che la sorveglianza e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti servono obiettivi legittimi connessi alla lotta contro il terrorismo.

35. Secondo questo stesso giudice, le rivelazioni fatte dal sig. Snowden hanno tuttavia dimostrato che la NSA e altri enti simili avevano commesso eccessi considerevoli. Sebbene la Foreign Intelligence Surveillance Court (in prosieguo: la «FISC»), la quale interviene nell'ambito della legge del 1978 sulla sorveglianza dei servizi di intelligence stranieri (Foreign Intelligence Surveillance Act of 1978[18]), eserciti una supervisione, il procedimento dinanzi alla medesima si svolgerebbe tuttavia segretamente e inaudita altera parte. Inoltre, a parte il fatto che le decisioni relative all'accesso ai dati personali verrebbero adottate sulla base del diritto americano, i cittadini dell'Unione non avrebbero alcun diritto effettivo ad essere sentiti sulla questione della sorveglianza e dell'intercettazione dei loro dati.

36. Emergerebbe chiaramente dai voluminosi documenti che corredano le dichiarazioni giurate rese nel procedimento principale che l'esattezza di una considerevole quantità delle rivelazioni del sig. Snowden non viene rimessa in discussione. La Corte d'appello ha pertanto concluso che, una volta che i dati personali vengono trasferiti negli Stati Uniti, la NSA nonché altre agenzie di sicurezza americane, come il Federal Bureau of Investigation (FBI) possono accedervi nel corso di operazioni di sorveglianza e intercettazioni di massa indiscriminate.

37. La Corte d'appello rileva che, nel diritto irlandese, l'importanza dei diritti costituzionali alla vita privata e all'inviolabilità del domicilio esige che qualsiasi ingerenza in tali diritti sia conforme ai requisiti previsti dalla legge e sia proporzionata. L'accesso massiccio e indiscriminato a dati personali non soddisferebbe affatto il requisito di proporzionalità e dovrebbe pertanto essere considerato contrario alla Costituzione irlandese[19].

38. La Corte d'appello rileva che, affinché intercettazioni di comunicazioni elettroniche possano essere considerate costituzionalmente legittime, occorrerebbe dimostrare che determinate intercettazioni di comunicazioni e la sorveglianza su talune persone o su taluni

[18] V. articolo 702 di tale legge, come modificata dalla legge del 2008 (Foreign Intelligence Surveillance Act of 2008). È in applicazione di tale articolo che la NSA detiene una banca dati conosciuta con il nome di «PRISM» (v. report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection del 27 novembre 2013).

[19] La Corte d'appello fa riferimento, in particolare, al rispetto della dignità umana e alla libertà della persona (preambolo), all'autonomia personale (articolo 40, paragrafo 3, punti 1 e 2), all'inviolabilità del domicilio (articolo 40, paragrafo 5) e alla protezione della vita familiare (articolo 41).

gruppi sono oggettivamente giustificate nell'interesse della sicurezza nazionale e della repressione della criminalità, e che esistono garanzie adeguate e verificabili.

39. Pertanto, la Corte d'appello indica che, se la presente causa dovesse essere trattata unicamente sulla base del diritto irlandese, si porrebbe un problema considerevole quanto alla questione se gli Stati Uniti «garantisc[a]no un livello adeguato di protezione della riservatezza e dei diritti e delle libertà fondamentali», ai sensi dell'articolo 11, paragrafo 1, della legge sulla protezione dei dati. Ne consegue che, sulla base del diritto irlandese, e in particolare dei suoi requisiti di carattere costituzionale, il commissario non avrebbe potuto respingere la denuncia del sig. Schrems, ma avrebbe dovuto esaminare tale questione.

40. Tuttavia, la Corte d'appello constata che la causa della quale è investita verte sull'attuazione del diritto dell'Unione ai sensi dell'articolo 51, paragrafo 1, della Carta, cosicché la legittimità della decisione del commissario dovrebbe essere valutata alla luce del diritto dell'Unione.

41. Il problema che il commissario ha dovuto affrontare viene spiegato dalla Corte d'appello nei seguenti termini. Ai sensi dell'articolo 11, paragrafo 2, lettera *a*) della legge sulla protezione dei dati, il commissario deve risolvere la questione dell'adeguatezza della protezione dei dati nello Stato terzo « in conformità » ad una constatazione dell'Unione effettuata dalla Commissione ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46. Ne consegue che il commissario non potrebbe discostarsi da una siffatta constatazione. Poiché la Commissione, nella sua decisione 2000/520, ha constatato che gli Stati Uniti garantiscono un livello di protezione adeguato quanto al trattamento dei dati da parte delle società che aderiscono ai principi dell'approdo sicuro, una denuncia che fa valere l'inadeguatezza di una siffatta protezione dovrebbe inevitabilmente essere respinta dal commissario.

42. Constatando al contempo che il commissario ha in tal modo dato prova di essersi scrupolosamente attenuto alla lettera della direttiva 95/46 e della decisione 2000/520, la Corte d'appello rileva che il sig. Schrems muove in realtà obiezioni nei confronti dei termini del regime dell'approdo sicuro stesso piuttosto che nei confronti del modo in cui il commissario l'ha applicato, sottolineando al contempo che egli non ha contestato direttamente la validità della direttiva 95/46 né quella della decisione 2000/520.

43. Secondo la Corte d'appello, la questione fondamentale sarebbe dunque se, alla luce del diritto dell'Unione e tenuto conto, in particolare, della successiva entrata in vigore degli articoli 7 e 8 della Carta, il commissario sia vincolato in maniera assoluta dalla constatazione della Commissione enunciata nella decisione 2000/520 in relazione all'adeguatezza del diritto e della prassi in materia di protezione dei dati personali negli Stati Uniti.

44. La Corte d'appello precisa inoltre che, nel ricorso del quale è investita, non è stata dedotta alcuna censura in ordine ai comportamenti di Facebook Ireland e di Facebook USA in quanto tali. Orbene, l'articolo 3, paragrafo 1, lettera *b*), della decisione 2000/520, il quale consente alle autorità nazionali competenti di ordinare ad un'impresa di sospendere i flussi di dati verso un paese terzo, si applicherebbe, secondo tale giudice, solo nei casi in cui la denuncia è diretta avverso la condotta dell'impresa di cui trattasi, il che non avverrebbe nel caso di specie.

45. La Corte d'appello sottolinea pertanto che la reale obiezione non riguarda la condotta di Facebook USA di per sé, bensì il fatto che la Commissione abbia ritenuto che il diritto e la prassi in materia di protezione dei dati negli Stati Uniti forniscano una protezione adeguata, mentre risulta chiaro, dalle rivelazioni del sig. Snowden, che i dati personali dei cittadini che vivono nel territorio dell'Unione sono accessibili alle autorità americane massicciamente e in maniera indifferenziata[20].

46. Su tale punto, la Corte d'appello ritiene che sia difficile immaginare come la decisione 2000/520 possa, nella prassi, soddisfare i requisiti degli articoli 7 e 8 della Carta, a maggior ragione alla luce dei principi elaborati dalla Corte nella sua sentenza Digital Rights Ireland e a[21]. In particolare, la garanzia prevista all'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni degli Stati membri sarebbe compromessa qualora si ammettesse che le comunicazioni elettroniche possano essere oggetto di accesso da parte delle autorità statali su base casuale e generalizzata, senza che sia richiesta una motivazione oggettiva in base a considerazioni di sicurezza nazionale o prevenzione di crimini specificamente riguardanti i singoli interessati, e senza la previsione di garanzie adeguate e verificabili. Poiché il ricorso del sig. Schrems suggerisce che la decisione 2000/520 potrebbe essere astrattamente incompatibile con gli articoli 7 e 8 della Carta, la Corte potrebbe ritenere che sia possibile interpretare la direttiva 95/46, e segnatamente il suo articolo 25, paragrafo 6, nonché la decisione 2000/520 in un senso che consenta alle autorità nazionali di condurre autonomamente indagini al fine di stabilire se il trasferimento di dati personali verso un paese terzo soddisfi i requisiti risultanti dagli articoli 7 e 8 della Carta.

47. In tale contesto, la Corte d'appello ha deciso di sospendere il procedimento e di sottoporre alla Corte le seguenti questioni pregiudiziali: «Se, nel decidere in merito a una denuncia presentata al commissario, secondo cui dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti) il cui diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, tenuto conto degli articoli 7, 8 e 47 della Carta, nonostante le disposizioni dell'articolo 25, paragrafo 6, della direttiva 95/46.
Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520».

II – Analisi

48. Le due questioni formulate dalla Corte d'appello invitano la Corte a precisare i poteri di cui dispongono le autorità nazionali di controllo allorché esse vengono investite di una denuncia concernente un trasferimento di dati personali verso un'impresa stabilita in un paese terzo e allorché viene dedotto, a sostegno di tale denuncia, che tale paese terzo non

[20] La Corte d'appello indica, a tal riguardo, che il motivo principale dedotto dal sig. Schrems dinanzi alla medesima consisteva nell'affermare che, alla luce delle recenti rivelazioni del sig. Snowden e del fatto che taluni dati personali sono stati messi a disposizione dei servizi di intelligence degli Stati Uniti su larga scala, il commissario non poteva trarre legittimamente la conclusione che, in tale paese terzo, esistesse un adeguato livello di protezione di detti dati.
[21] C - 2 9 3 / 1 2 e C - 5 9 4 / 1 2 , EU:C:2014:238, punti da 65 a 69.

garantisce un livello di protezione adeguato ai dati trasferiti, sebbene la Commissione abbia adottato, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, una decisione che riconosce l'adeguatezza del livello di protezione assicurato da detto paese terzo.

49. Osservo che la denuncia depositata dal sig. Schrems presso il commissario è caratterizzata da una duplice dimensione. Essa è intesa a contestare il trasferimento di dati personali da Facebook Ireland a Facebook USA. Il sig. Schrems chiede la cessazione di tale trasferimento poiché, a suo avviso, gli Stati Uniti non assicurerebbero un livello di protezione adeguato ai dati personali che vengono trasferiti nell'ambito del regime dell'approdo sicuro. Più precisamente, a tale paese terzo è addebitata la creazione del programma PRISM, il quale consente alla NSA di accedere liberamente ai dati conservati in massa in server ubicati negli Stati Uniti. In tal senso, la denuncia ha specificamente ad oggetto i trasferimenti di dati personali da Facebook Ireland a Facebook USA, mettendo al contempo in discussione in maniera più generale il livello di protezione assicurato a tali dati nell'ambito del regime approdo sicuro.

50. Il commissario ha ritenuto che l'esistenza stessa di una decisione della Commissione che riconosce che gli Stati Uniti assicurano, nell'ambito del regime dell'approdo sicuro, un livello di protezione adeguato, gli impedisse di istruire la denuncia.

51. Occorre pertanto esaminare congiuntamente le due questioni, con le quali si chiede, in sostanza, se l'articolo 28 della direttiva 95/46, in combinato disposto con gli articoli 7 e 8 della Carta, debba essere interpretato nel senso che l'esistenza di una decisione adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, di questa direttiva produca l'effetto di impedire ad un'autorità nazionale di controllo di istruire una denuncia con la quale lamenta che un paese terzo non assicura un livello di protezione adeguato ai dati personali trasferiti e, se del caso, di sospendere il trasferimento di tali dati.

52. L'articolo 7 della Carta garantisce il diritto al rispetto della vita privata, mentre il suo articolo 8 proclama espressamente il diritto alla protezione dei dati di carattere personale. I paragrafi 2 e 3 di quest'ultimo articolo precisano che tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica e che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

A - *Sui poteri delle autorità nazionali di controllo in caso di decisione della Commissione che dichiara l'adeguatezza*

53. Come indicato dal sig. Schrems nelle sue osservazioni, ai fini della denuncia di cui al procedimento principale, la questione centrale concerne il trasferimento di dati personali da Facebook Ireland a Facebook USA alla luce dell'accesso generalizzato, da parte della NSA e di altre agenzie di sicurezza americane, ai dati conservati presso Facebook USA in forza dei poteri loro conferiti dalla legislazione americana.

54. Quando è investita di una denuncia intesa a rimettere in discussione la constatazione secondo la quale un paese terzo garantisce un livello di protezione adeguato ai dati trasferiti, secondo il sig. Schrems l'autorità nazionale di controllo ha il potere, qualora disponga di elementi che depongono nel senso della fondatezza delle allegazioni contenute in tale denuncia, di ordinare la sospensione del trasferimento di dati effettuato dall'impresa de-

signata in detta denuncia.

55. Alla luce degli obblighi del commissario di proteggere i diritti fondamentali del sig. Schrems, quest'ultimo sostiene che il commissario è tenuto non solo ad indagare, bensì anche, in caso di accoglimento della denuncia, ad utilizzare i propri poteri per sospendere il flusso di dati fra Facebook Ireland e Facebook USA.

56. Orbene, il commissario ha respinto la denuncia sulla base delle disposizioni della legge sulla protezione dei dati che elencano i suoi poteri. Tale conclusione era fondata sulla convinzione del commissario di essere vincolato dalla decisione 2000/520.

57. Ne consegue che la questione centrale nella presente causa è di chiarire se la valutazione della Commissione sull'adeguatezza del livello di protezione, contenuta nella decisione 2000/520, vincoli in maniera assoluta l'autorità nazionale di protezione dei dati e le impedisca di indagare su affermazioni intese a rimettere in discussione tale constatazione. Le questioni pregiudiziali vertono dunque sulla portata dei poteri di indagine delle autorità nazionali di protezione dei dati quando la Commissione ha emanato una decisione che dichiara l'adeguatezza.

58. Secondo la Commissione, occorre tenere conto del rapporto fra i poteri della medesima e quelli delle autorità nazionali di protezione dei dati. Le competenze di queste ultime sarebbero focalizzate sull'applicazione della normativa in tale materia in singoli casi, mentre il riesame generale dell'applicazione della decisione 2000/520, inclusa ogni decisione che ne comporta la sospensione o l'abrogazione, rientrerebbe nella competenza della Commissione.

59. La Commissione fa valere che il sig. Schrems non avrebbe dedotto argomenti specifici che inducano a pensare che lo stesso correva un rischio imminente di subire danni gravi a causa del trasferimento di dati fra Facebook Ireland e Facebook USA. Al contrario, a causa della loro natura astratta e generale, le preoccupazioni espresse dal sig. Schrems a proposito dei programmi di sorveglianza attuati dalle agenzie di sicurezza americane sarebbero identiche a quelle che hanno condotto la Commissione ad avviare il riesame della decisione 2000/520.

60. Secondo la Commissione, le autorità nazionali di controllo interferirebbero nelle competenze di cui essa dispone per rinegoziare le condizioni di tale decisione con gli Stati Uniti o, se necessario, per sospenderla, qualora adottassero misure sulla base di denunce che si limitano ad enunciare preoccupazioni strutturali ed astratte.

61. Non condivido l'opinione della Commissione. A mio avviso, l'esistenza di una decisione adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46 non può elidere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza dell'articolo 28 di tale direttiva. Contrariamente a quanto afferma la Commissione, se le autorità nazionali di controllo vengono adite nell'ambito di denunce individuali, ciò non impedisce loro, a mio avviso, in forza dei loro poteri di indagine e della loro indipendenza, di formarsi un'opinione autonoma sul livello generale di protezione assicurato da un paese terzo e di trarne le conseguenze allorché esse statuiscono su singoli casi concreti.

62. Discende da costante giurisprudenza della Corte che, ai fini dell'interpretazione delle disposizioni di diritto dell'Unione, si deve tener conto non soltanto della lettera delle stesse, ma anche del loro contesto e degli scopi perseguiti dalla normativa di cui esse fanno parte[22].

63. Risulta dal considerando 62 della direttiva 95/46 che « la designazione di autorità di controllo che agiscano in modo indipendente in ciascuno Stato membro è un elemento essenziale per la tutela delle persone con riguardo al trattamento di dati personali ».

64. Ai sensi dell'articolo 28, paragrafo 1, primo comma, di tale direttiva, «[o]gni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l'applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri». L'articolo 28, paragrafo 1, secondo comma, di detta direttiva dispone che «[t]ali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite».

65. L'articolo 28, paragrafo 3, della direttiva 95/46 elenca i poteri di cui ogni autorità di controllo dispone, vale a dire poteri investigativi, poteri effettivi d'intervento che le consentono, segnatamente, di vietare a titolo provvisorio o definitivo un trattamento, nonché il potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione di tale direttiva ovvero di adire per dette violazioni le autorità giudiziarie.

66. Inoltre, ai sensi dell'articolo 28, paragrafo 4, primo comma, della direttiva 95/46, «[q]ualsiasi persona […] può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali». L'articolo 28, paragrafo 4, secondo comma, di tale direttiva, precisa che «[q]ualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 [di detta] direttiva». Preciso che quest'ultima disposizione consente agli Stati membri di adottare misure di legge intese a limitare la portata di diversi obblighi e diritti previsti nella direttiva 95/46, qualora tale restrizione costituisca una misura necessaria alla salvaguardia, segnatamente, della sicurezza dello Stato, della difesa, della pubblica sicurezza, nonché della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali.

67. Come già rilevato dalla Corte, l'esigenza di un controllo, da parte di un'autorità indipendente, dell'osservanza delle norme del diritto dell'Unione relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali risulta altresì dal diritto primario dell'Unione, segnatamente dall'articolo 8, paragrafo 3, della Carta e dall'articolo 16, paragrafo 2, TFUE[23]. Essa ha parimenti rammentato che «[l]'istituzione, negli Stati membri, di autorità di controllo indipendenti costituisce quindi un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali[24]».

---

[22] V., segnatamente, sentenza Koushkaki (C-84/12, EU:C:2013:862, punto 34 e la giurisprudenza ivi citata).

[23] V. sentenze Commissione/Austria (C-614/10, EU:C:2012:631, punto 36) e Commissione/ Ungheria (C - 2 8 8 / 1 2 , EU:C:2014:237, punto 47).

[24] V., segnatamente, sentenze Commissione/Ungheria (C-288/12, EU:C:2014:237, punto 48 e la giurisprudenza ivi citata). V. parimenti, in tal senso, la sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 68, nonché la giuri-

68. La Corte ha anche statuito che «l'articolo 28, paragrafo 1, secondo comma, della direttiva 95/46 deve essere interpretato nel senso che le autorità di controllo competenti per la vigilanza del trattamento dei dati personali devono godere di un'indipendenza che consenta loro di svolgere le proprie funzioni senza subire influenze esterne. Tale indipendenza esclude in particolare qualsiasi imposizione e ogni altra influenza esterna di qualunque forma, sia diretta che indiretta, che possano orientare le loro decisioni e che potrebbero quindi rimettere in discussione lo svolgimento, da parte di dette autorità, del loro compito, consistente nello stabilire un giusto equilibrio tra la protezione del diritto alla vita privata e la libera circolazione dei dati personali[25]».

69. La Corte ha parimenti precisato che «[l]a garanzia dell'indipendenza delle autorità nazionali di controllo è diretta ad assicurare l'efficacia e l'affidabilità del controllo del rispetto delle disposizioni in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali[26]». Tale garanzia d'indipendenza è stata disposta « per rafforzare la protezione delle persone e degli organismi interessati dalle […] decisioni [di tali autorità nazionali di controllo][27]».

70. Come emerge in particolare dal considerando 10 e dall'articolo 1 della direttiva 95/46, essa si propone di garantire, all'interno dell'Unione, « un elevato grado di tutela delle libertà e dei diritti fondamentali con riguardo al trattamento dei dati personali[28]». Secondo la Corte, «[l]e autorità di controllo previste all'art[icolo] 28 della direttiva 95/46 sono quindi le custodi dei menzionati diritti e libertà fondamentali[29]».

71. Tenuto conto dell'importanza del ruolo svolto dalle autorità nazionali di controllo in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, i loro poteri di intervento devono permanere anche quando la Commissione ha adottato una decisione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46.

72. Osservo, a tal riguardo, che nulla indica che i regimi di trasferimento di dati personali verso paesi terzi siano esclusi dall'ambito di applicazione ratione materiae dell'articolo 8, paragrafo 3, della Carta, il quale consacra al livello più alto della gerarchia delle norme nel diritto dell'Unione l'importanza del controllo esercitato da un'autorità indipendente per quanto attiene al rispetto delle norme relative alla protezione dei dati personali.

73. Se le autorità nazionali di controllo fossero vincolate in maniera assoluta dalle decisioni adottate dalla Commissione, ciò limiterebbe inevitabilmente la loro totale indipendenza. In conformità al loro ruolo di custodi dei diritti fondamentali, le autorità nazionali di controllo devono poter indagare, in piena indipendenza, sui reclami loro sottoposti,

---

sprudenza ivi citata).

[25] V., segnatamente, sentenza Commissione/Ungheria (C- 288/12 , EU:C:2014:237, punto 51 e la giurisprudenza ivi citata).

[26] Sentenza Commissione/Germania (C-518/07, EU:C:2010:125, punto 25).

[27] *Idem*

[28] *Ibidem* (punto 22 e la giurisprudenza ivi citata).

[29] *Ibidem* (punto 23). V., parimenti, in tal senso, sentenze Commissione/Austria (C-614/10, EU:C:2012:631, punto 52) e Comm iss ione/U nghe ria (C-288/12 , EU:C:2014:237, punto 53).

nell'interesse superiore della protezione dei singoli con riguardo al trattamento dei dati personali.

74. Inoltre, come rilevato giustamente dal governo belga e dal Parlamento europeo in udienza, non esiste alcun vincolo gerarchico fra il capo IV della direttiva 95/46, relativo al trasferimento di dati personali verso paesi terzi, e il capo VI della medesima, il quale è dedicato, segnatamente, al ruolo delle autorità nazionali di controllo. Nulla, nel capo VI, suggerisce che le disposizioni relative alle autorità nazionali di controllo siano subordinate in una qualsivoglia maniera alle disposizioni distinte sui trasferimenti enunciate nel capo IV della direttiva 95/46.

75. Al contrario, risulta in maniera esplicita dall'articolo 25, paragrafo 1, di tale direttiva, figurante al capo IV della medesima, che l'autorizzazione del trasferimento di dati personali verso un paese terzo che garantisce un livello di protezione adeguato vale solo fatte salve le misure nazionali di attuazione delle altre disposizioni di detta direttiva.

76. Ricordo, a tal riguardo, che, in forza di tale disposizione, gli Stati membri devono prevedere, nella loro legislazione nazionale, che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento, può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della direttiva 95/46.

77. Ai sensi dell'articolo 28, paragrafo 1, di tale direttiva, le autorità nazionali di controllo sono incaricate di sorvegliare, nel territorio di ciascuno Stato membro, l'applicazione delle disposizioni di attuazione di detta direttiva, adottate dagli Stati membri.

78. L'accostamento fra queste due disposizioni consente di ritenere che la regola enunciata all'articolo 25, paragrafo 1, della direttiva 95/46, secondo la quale il trasferimento di dati personali può aver luogo soltanto se il paese terzo destinatario garantisce loro un livello di protezione adeguato, faccia parte delle regole di cui le autorità nazionali di controllo devono sorvegliare l'applicazione.

79. Occorre interpretare estensivamente, in conformità all'articolo 8, paragrafo 3, della Carta, i poteri delle autorità nazionali di controllo di indagare in completa indipendenza sui reclami di cui esse vengono investite ai sensi dell'articolo 28 della direttiva 95/46. Tali poteri non possono pertanto essere limitati dai poteri conferiti dal legislatore dell'Unione alla Commissione, ai sensi dell'articolo 25, paragrafo 6, di tale direttiva, al fine di accertare l'adeguatezza del livello di protezione offerto da un paese terzo.

80. Alla luce del loro ruolo fondamentale in materia di protezione dei dati personali, le autorità nazionali di controllo devono poter indagare allorché esse vengono investite di una denuncia che indica elementi che potrebbero essere in grado di rimettere in discussione il livello di protezione assicurato da un paese terzo, incluso il caso in cui la Commissione ha constatato, in una decisione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, che il paese terzo interessato assicura un livello di protezione adeguato.

81. Se, al termine delle indagini condotte da un'autorità nazionale di controllo, essa ritiene che il trasferimento di dati contestato arrechi pregiudizio alla protezione di cui

devono beneficiare i cittadini dell'Unione quanto al trattamento dei loro dati, essa ha il potere di sospendere il trasferimento di dati in parola, e ciò a prescindere dalla valutazione generale effettuata dalla Commissione nella sua decisione. 82. È infatti pacifico, ai sensi dell'articolo 25, paragrafo 2, della direttiva 95/46, che l'adeguatezza del livello di protezione offerto da un paese terzo viene valutata in funzione di un insieme di circostanze sia di fatto che di diritto. Se una di tali circostanze muta e risulta idonea a rimettere in discussione l'adeguatezza del livello di protezione offerto da un paese terzo, l'autorità nazionale di controllo investita di una denuncia deve poterne trarre le conseguenze rispetto al trasferimento contestato.

83. Effettivamente, come rilevato dall'Irlanda, il commissario, al pari delle altre autorità statali, è vincolato dalla decisione 2000/520. Risulta infatti dall'articolo 288, quarto comma, TFUE, che una decisione adottata da un'istituzione dell'Unione è obbligatoria in tutti i suoi elementi. Di conseguenza, la decisione 2000/520 vincola gli Stati membri ai quali è destinata.

84. Rilevo, a tal riguardo, che la stessa decisione 2000/520 dispone, al suo articolo 5, che «[g]li Stati membri adottano le misure necessarie per conformarsi alla [medesima] entro 90 giorni dalla data di notifica delle stesse». Inoltre, l'articolo 6 di tale decisione conferma che «[g]li Stati membri sono destinatari della [stessa]».

85. Tuttavia ritengo che, alla luce delle summenzionate disposizioni della direttiva 95/46 e della Carta, l'effetto vincolante della decisione 2000/520 non sia idoneo ad escludere qualsiasi indagine del commissario su denunce con le quali si fa valere che trasferimenti di dati personali effettuati verso gli Stati Uniti nell'ambito di tale decisione non presentano le garanzie necessarie di protezione richieste dal diritto dell'Unione. In altre parole, un siffatto effetto vincolante non implica che ogni denuncia di questo tipo debba essere respinta sommariamente, ossia immediatamente e senza alcun esame della sua fondatezza.

86. Aggiungo che si evince inoltre dall'impianto dell'articolo 25 della direttiva 95/46 che l'accertamento se un paese terzo assicuri o meno un livello di protezione adeguato può essere effettuato vuoi dagli Stati membri vuoi dalla Commissione. Si tratta pertanto di una competenza ripartita.

87. Risulta dall'articolo 25, paragrafo 6, di tale direttiva che, qualora la Commissione constati che un paese terzo garantisce un livello di protezione adeguato, ai sensi dell'articolo 25, paragrafo 2, di detta direttiva, gli Stati membri devono adottare le misure necessarie per conformarsi alla decisione della Commissione.

88. Dato che una siffatta decisione produce l'effetto di consentire i trasferimenti di dati personali verso un paese terzo il cui livello di protezione è considerato adeguato dalla Commissione, gli Stati membri devono quindi consentire, in linea di principio, che siffatti trasferimenti siano effettuati dalle imprese stabilite nel loro territorio.
89. L'articolo 25 della direttiva 95/46 non attribuisce tuttavia alla Commissione una competenza esclusiva in materia di accertamento dell'adeguatezza o meno del livello di protezione dei dati personali trasferiti. L'impianto di tale articolo dimostra che gli Stati membri ricoprono parimenti un ruolo in materia. È vero che una decisione della Commissione svolge un ruolo importante per l'uniformazione delle condizioni di trasferimento valide all'interno degli Stati membri. Tuttavia, tale uniformazione può perdurare solo

fintantoché tale accertamento non venga messo in discussione.

90. L'argomento della necessaria uniformazione delle condizioni di trasferimento dei dati personali verso un paese terzo trova il proprio limite, a mio avviso, in una situazione come quella di cui al procedimento principale, nella quale non solo la Commissione è al corrente del fatto che la sua constatazione è soggetta a critiche, ma è anche essa stessa che formula siffatte critiche e conduce negoziati per porvi rimedio.

91. La valutazione dell'adeguatezza o meno del livello della protezione offerto da un paese terzo può parimenti sfociare in una cooperazione fra gli Stati membri e la Commissione. L'articolo 25, paragrafo 3, della direttiva 95/46 prevede, a tal riguardo, che «[g]li Stati membri e la Commissione si comunicano a vicenda i casi in cui, a loro parere, un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2». Come osservato dal Parlamento, ciò dimostra chiaramente che gli Stati membri e la Commissione devono svolgere un ruolo equivalente per individuare i casi in cui un paese terzo non assicura un livello di protezione adeguato.

92. La decisione di adeguatezza è intesa ad autorizzare il trasferimento di dati personali verso il paese terzo interessato. Ciò non implica che le autorità di controllo non possano più essere investite dai cittadini dell'Unione di una domanda volta a proteggere i loro dati personali. Osservo, a tal riguardo, che l'articolo 28, paragrafo 4, primo comma, della direttiva 95/46, secondo il quale «[q]ualsiasi persona […] può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali», non prevede eccezioni a tale principio in caso di esistenza di una decisione adottata dalla Commissione in applicazione dell'articolo 25, paragrafo 6, di tale direttiva.

93. Pertanto, se una decisione adottata dalla Commissione in applicazione dei poteri esecutivi che le sono conferiti da quest'ultima disposizione ha l'effetto di consentire il trasferimento di dati personali verso un paese terzo, una siffatta decisione non può avere come effetto, per contro, di togliere ogni potere agli Stati membri, e in particolare alle loro autorità nazionali di controllo, o anche soltanto di restringere le loro competenze, allorché esse si trovano di fronte ad affermazioni di violazioni di diritti fondamentali.

94. Un'autorità nazionale di controllo deve essere in grado di esercitare i poteri previsti all'articolo 28, paragrafo 3, della direttiva 95/46, fra cui quello di vietare a titolo provvisorio o definitivo un trattamento di dati personali. Pur se l'elencazione dei poteri, prevista a tale disposizione, non prevede esplicitamente poteri relativi ad un trasferimento da uno Stato membro verso un paese terzo, si deve ritenere, a mio avviso, che un siffatto trasferimento costituisca un trattamento di dati[30]. Come si evince dal testo di detta disposizione, l'elencazione non è, inoltre, esaustiva. In ogni caso, alla luce del ruolo fondamentale svolto dalle autorità nazionali di controllo nel sistema predisposto dalla direttiva 95/46, esse devono disporre del potere di sospendere un trasferimento di dati in caso di violazione effettiva o potenziale dei diritti fondamentali.

[30] V. conclusioni dell'avvocato generale Léger nella causa Parlamento/Consiglio e Commissione (C-317/04, EU:C:2005:710, paragrafi da 92 a 95). V., parimenti, sentenza Parlamento/Consiglio e Commissione (C-317/04 e C-318/04, EU:C:2006:346, punto 56).

95. Aggiungo che privare l'autorità nazionale di controllo dei suoi poteri di indagine in circostanze come quelle di cui alla presente causa sarebbe contrario non solo al principio di indipendenza, ma anche all'obiettivo della direttiva 95/46, quale risulta dall'articolo 1, paragrafo 1, della stessa.

96. Come rilevato dalla Corte, «[r]isulta dai considerando 3, 8 e 10 della direttiva 95/46 che il legislatore dell'Unione ha inteso facilitare la libera circolazione dei dati personali ravvicinando le legislazioni degli Stati membri pur salvaguardando i diritti fondamentali della persona, in particolare il diritto alla tutela della vita privata, e garantendo un elevato grado di tutela nell'Unione. L'articolo 1 di tale direttiva prevede infatti che gli Stati membri debbano garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche, in particolare della loro vita privata, con riguardo al trattamento dei dati personali[31]».

97. Le disposizioni della direttiva 95/46 devono pertanto essere interpretate in conformità all'obiettivo della medesima, consistente nel garantire un livello elevato di protezione delle libertà e dei diritti fondamentali delle persone fisiche, e segnatamente della loro vita privata, con riguardo al trattamento dei dati personali all'interno dell'Unione.

98. L'importanza di tale obiettivo e il ruolo che gli Stati membri devono svolgere per conseguirlo implicano che, qualora circostanze particolari vengano a fondare un dubbio serio quanto al rispetto dei diritti fondamentali garantiti dalla Carta in caso di trasferimento di dati personali verso un paese terzo, gli Stati membri e dunque, al loro interno, le autorità nazionali di controllo, non possono essere vincolati in maniera assoluta da una decisione di adeguatezza della Commissione.

99. La Corte ha già statuito che «le disposizioni della direttiva 95/46, disciplinando il trattamento di dati personali che possono arrecare pregiudizio alle libertà fondamentali e, segnatamente, al diritto alla vita privata, devono necessariamente essere interpretate alla luce dei diritti fondamentali che, secondo una costante giurisprudenza, formano parte integrante dei principi generali del diritto di cui la Corte garantisce l'osservanza e che sono ormai iscritti nella Carta[32]».

100. Mi riferisco, inoltre, alla giurisprudenza secondo la quale «gli Stati membri sono tenuti non solo a interpretare il loro diritto nazionale conformemente al diritto dell'Unione, ma anche a fare in modo di non basarsi su un'interpretazione di norme di diritto derivato che entri in conflitto con i diritti fondamentali tutelati dall'ordinamento giuridico dell'Unione o con gli altri principi generali del diritto dell'Unione[33]».

101. La Corte ha in tal senso statuito, nella sua sentenza N.S. e a.[34], che «un'applicazione del regolamento [(CE)] n. 343/2003[35] sulla base di una presunzione assoluta che i diritti

[31] V., segnatamente, sentenza IPI (C-473/12, EU:C:2013:715, punto 28 e la giurisprudenza ivi citata).
[32] V., segnatamente, sentenza Google Spain e Google (C-131/12, EU:C:2014:317, punto 68 e la giurisprudenza ivi citata).
[33] V., segnatamente, sentenza N.S. e a. (C-411/10 e C-493/10, EU:C:2011:865, punto 77, nonché la giurisprudenza ivi citata).
[34] C-411/10 e C-493/10 , EU:C:2011:865.
[35] Regolamento del Consiglio del 18 febbraio 2003, che stabilisce i criteri e i meccanismi

fondamentali del richiedente asilo saranno rispettati nello Stato membro di regola competente a conoscere della sua domanda è incompatibile con l'obbligo degli Stati membri di interpretare e di applicare il regolamento n. 343/2003 in conformità ai diritti fondamentali[36]».

102. A tal riguardo, la Corte ha ammesso, laddove si trattava dello status degli Stati membri quali paesi di origine reciprocamente sicuri a tutti i fini giuridici e pratici connessi a questioni inerenti l'asilo, che si deve presumere che il trattamento riservato ai richiedenti asilo in ciascuno Stato membro sia conforme a quanto prescritto dalla Carta, alla Convenzione relativa allo status dei rifugiati, firmata a Ginevra il 28 luglio 1951[37], nonché alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950[38]. Tuttavia, la Corte ha dichiarato che «non si può escludere che tale sistema incontri, in pratica, gravi difficoltà di funzionamento in un determinato Stato membro, cosicché sussiste un rischio serio che un richiedente asilo sia, in caso di trasferimento verso detto Stato membro, trattato in modo incompatibile con i suoi diritti fondamentali[39]».

103. Di conseguenza, la Corte ha statuito che «gli Stati membri, compresi gli organi giurisdizionali nazionali, sono tenuti a non trasferire un richiedente asilo verso lo "Stato membro competente" ai sensi del regolamento n. 343/2003 quando non possono ignorare che le carenze sistemiche nella procedura di asilo e nelle condizioni di accoglienza dei richiedenti asilo in tale Stato membro costituiscono motivi seri e comprovati di credere che il richiedente corra un rischio reale di subire trattamenti inumani o degradanti ai sensi dell'art[icolo] 4 della Carta[40]».

104. Mi sembra che l'apporto della sentenza N.S. e a.[41] possa essere esteso ad una situazione come quella di cui al procedimento principale. In tal senso, un'interpretazione del diritto derivato dell'Unione che poggi su una presunzione assoluta che i diritti fondamentali saranno rispettati — indifferentemente, da parte di uno Stato membro, dalla Commissione o da un paese terzo—deve essere considerata incompatibile con l'obbligo degli Stati membri di interpretare e applicare il diritto derivato dell'Unione in maniera conforme ai diritti fondamentali. L'articolo 25, paragrafo 6, della direttiva 95/46 non sancisce pertanto una siffatta presunzione assoluta di rispetto dei diritti fondamentali per quanto attiene alla valutazione, a parte della Commissione, dell'adeguatezza del livello di protezione offerto da un paese terzo. Al contrario, la presunzione, sottesa a tale disposizione, secondo la quale il trasferimento di dati verso un paese terzo rispetta i diritti fondamentali, deve essere considerata relativa[42]. Di conseguenza, detta disposizione non dovrebbe essere interpretata nel senso che essa rimette in discussione le garanzie figuranti segnatamente all'articolo 28, paragrafo 3, della direttiva 95/46 e all'articolo 8, paragrafo 3, della Carta,

---

di determinazione dello Stato membro competente per l'esame di una domanda d'asilo presentata in uno degli Stati membri da un cittadino di un paese terzo (GU L 50, pag. 1).

[36] Punto 99 di tale sentenza.

[37] *Recueil des traités des Nations unies*, vol. 189, pag. 150, n. 2545 (1954).

[38] V. sentenza N.S. e a. (C-411/10 e C-493/10, EU:C:2011:865, punto 80).

[39] *Ibidem* (punto 81).

[40] *Ibidem* (punto 94).

[41] C-411/10 e C-493/1 0 , EU:C:2011:865.

[42] Punto 104 di tale sentenza

intesi alla protezione e al rispetto del diritto alla protezione dei dati personali.

105. Deduco pertanto dalla detta sentenza che, in caso di carenze sistemiche constatate nel paese terzo verso il quale vengono trasferiti dati personali, gli Stati membri devono poter adottare le misure necessarie alla salvaguardia dei diritti fondamentali protetti dagli articoli 7 e 8 della Carta.

106. Inoltre, come rilevato dal governo italiano nelle sue osservazioni, l'adozione, da parte della Commissione, di una decisione di adeguatezza non può produrre l'effetto di ridurre la protezione dei cittadini dell'Unione con riguardo al trattamento dei loro dati allorché questi ultimi vengono trasferiti verso un paese terzo, rispetto al livello di protezione di cui tali persone beneficerebbero se i loro dati fossero oggetto di un trattamento all'interno dell'Unione. Le autorità nazionali di controllo devono pertanto essere in grado di intervenire e di esercitare i loro poteri nei confronti di trasferimenti di dati verso paesi terzi oggetto di una decisione sull'adeguatezza. In caso contrario, i cittadini dell'Unione godrebbero di una protezione inferiore che nel caso di trattamento dei loro dati all'interno dell'Unione.

107. Pertanto, l'adozione, da parte della Commissione, di una decisione in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46 ha come unico effetto la rimozione del divieto generale di esportazione dei dati personali verso paesi terzi che garantiscono un livello di protezione comparabile a quello offerto da tale direttiva. In altre parole, non si tratta di creare un regime speciale derogatorio e meno protettivo per i cittadini dell'Unione rispetto al regime generale previsto da detta direttiva per i trattamenti di dati che vengono effettuati all'interno dell'Unione.

108. È vero che la Corte ha indicato, al punto 63 della sentenza Lindqvist[43], che «[i]l capo IV della direttiva 95/46, nel quale figura l'art[icolo] 25, predispone un regime speciale». Tuttavia, ciò non significa, a mio avviso, che un siffatto regime debba essere meno protettivo. Al contrario, al fine di conseguire l'obiettivo di protezione dei dati fissato all'articolo 1, paragrafo 1, della direttiva 95/46, l'articolo 25 della medesima impone vari obblighi agli Stati membri e alla Commissione[44], e tale articolo 25 sancisce il principio secondo il quale, quando un paese terzo non offre un livello di protezione adeguato, il trasferimento di dati personali verso tale paese dev'essere vietato[45].

109. Per quanto attiene più specificamente al regime dell'approdo sicuro, la Commissione prevede l'intervento delle autorità nazionali di controllo e la sospensione, da parte delle medesime, dei flussi di dati, solo nell'ambito tracciato dall'articolo 3, paragrafo 1, lettera *b*), della decisione 2000/520.

110. Secondo il considerando 8 di tale decisione, « [n]ell'interesse della trasparenza, e per salvaguardare la facoltà delle competenti autorità degli Stati membri di assicurare la protezione degli individui riguardo al trattamento dei dati personali, è necessario che la presente decisione specifichi le circostanze eccezionali in cui può essere giustificata la sospensione di specifici flussi di dati anche in caso di constatazione di adeguata protezione».

[43] C-101/01, EU:C:2003:596.
[44] Punto 65.
[45] Punto 64.

111. Nell'ambito della presente causa, è più in particolare l'applicazione dell'articolo 3, paragrafo 1, lettera *b*), di detta decisione che è stata discussa. In tal senso, in forza di tale disposizione, le autorità nazionali di controllo possono decidere di sospendere flussi di dati nei casi in cui «sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare».

112. Detta disposizione pone varie condizioni che hanno formato oggetto di diverse interpretazioni ad opera delle parti nel corso del presente procedimento[46]. Senza entrare nel dettaglio di tali interpretazioni, ne emerge che tali condizioni regolano in maniera restrittiva il potere delle autorità nazionali di controllo di sospendere flussi di dati.

113. Orbene, contrariamente a quanto fatto valere dalla Commissione, l'articolo 3, paragrafo 1, lettera *b*), della decisione 2000/520 deve essere interpretato in conformità all'obiettivo di protezione dei dati personali perseguito dalla direttiva 95/46, nonché alla luce dell'articolo 8 della Carta. La necessità di un'interpretazione conforme ai diritti fondamentali milita a favore di un'interpretazione estensiva di tale disposizione.

114. Ne consegue che le condizioni previste all'articolo 3, paragrafo 1 lettera *b*), della decisione 2000/520 non possono, a mio avviso, impedire ad un'autorità nazionale di controllo di esercitare in piena indipendenza i poteri di cui è investita in forza dell'articolo 28, paragrafo 3, della direttiva 95/46.

115. Come indicato in sostanza dai governi belga e austriaco in udienza, l'uscita di emergenza costituita dall'articolo 3, paragrafo 1, lettera *b*), della decisione 2000/520 è talmente stretta che è difficile sfruttarla. Essa impone criteri cumulativi ed è eccessivamente esigente. Orbene, alla luce dell'articolo 8, paragrafo 3, della Carta, è impossibile che il potere discrezionale delle autorità nazionali di controllo concernente le prerogative che risultano dall'articolo 28, paragrafo 3, della direttiva 95/46 sia a tal punto limitato che esse non possano più essere esercitate.

116. A tal riguardo, il Parlamento ha giustamente osservato che è il legislatore dell'Unione ad avere deciso quali fossero i poteri che dovevano spettare alle autorità nazionali di controllo. Orbene, il potere di esecuzione accordato dal legislatore dell'Unione alla Commissione all'articolo 25, paragrafo 6, della direttiva 95/46 non pregiudica i poteri conferiti da questo stesso legislatore alle autorità nazionali di controllo all'articolo 28, paragrafo 3, di tale direttiva. In altre parole, la Commissione non è competente a restringere i poteri

[46] Secondo il sig. Schrems, la prima condizione, secondo la quale «sia molto probabile che i principi vengano violati», non sarebbe soddisfatta. Orbene, non viene dedotto che Facebook USA, quale organismo autocertificato al quale vengono trasferiti dati, avrebbe essa stessa violato i principi dell'approdo sicuro a causa dell'accesso massiccio e indifferenziato da parte delle autorità americane ai dati da essa detenuti. Infatti, i principi dell'approdo sicuro sono espressamente limitati dal diritto americano, che l'allegato I, quarto comma, della decisione 2000/520 definisce rimandando alle disposizioni legislative o regolamentari e alle decisioni giurisdizionali.

delle autorità nazionali di controllo.

117. Di conseguenza, al fine di assicurare una protezione adeguata dei diritti fondamentali delle persone fisiche con riguardo al trattamento dei dati personali, le autorità nazionali di controllo devono essere autorizzate, qualora vengano dedotte violazioni di tali diritti, a condurre indagini. Se, al termine di tali indagini, dette autorità ritengono che esistano, in un paese terzo coperto da una decisione di adeguatezza, indizi seri di una violazione del diritto dei cittadini dell'Unione alla protezione dei loro dati personali, esse devono poter sospendere il trasferimento di dati verso il destinatario stabilito in tale paese terzo.

118. In altre parole, le autorità nazionali di controllo devono poter condurre le loro indagini e, se del caso, sospendere un trasferimento di dati, a prescindere dalle condizioni restrittive fissate all'articolo 3, paragrafo 1, lettera *b*), della decisione 2000/520.

119. Inoltre, in forza del loro potere di promuovere azioni giudiziarie in caso di violazioni delle disposizioni nazionali di attuazione della direttiva 95/46 ovvero del loro potere di adire per dette violazioni le autorità giudiziarie, ai sensi dell'articolo 28, paragrafo 3, di tale direttiva, le autorità nazionali di controllo, qualora vengano a conoscenza di fatti che dimostrano che un paese terzo non assicura un livello di protezione adeguato, dovrebbero poter adire un giudice nazionale il quale potrà esso stesso decidere, se del caso, di effettuare un rinvio pregiudiziale alla Corte ai fini della valutazione della validità di una decisione sull'adeguatezza della Commissione.

120. Risulta dall'insieme di tali elementi che l'articolo 28 della direttiva 95/46, in combinato disposto con gli articoli 7 e 8 della Carta, deve essere interpretato nel senso che l'esistenza di una decisione adottata dalla Commissione sulla base dell'articolo 25, paragrafo 6, di tale direttiva non produce l'effetto di impedire ad un'autorità nazionale di controllo di istruire una denuncia con la quale si lamenta che un paese terzo non assicura un livello di protezione adeguato ai dati personali trasferiti e, se del caso, di sospendere il trasferimento di tali dati.

121. Anche se la Corte d'appello sottolinea, nella sua decisione di rinvio, che il sig. Schrems non ha formalmente contestato, nel ricorso principale, né la validità della direttiva 95/46 né quella della decisione 2000/520, si evince da tale decisione di rinvio che la censura principale mossa dal sig. Schrems è intesa a rimettere in discussione l'affermazione secondo la quale gli Stati Uniti assicurano, nell'ambito del regime dell'approdo sicuro, un livello di protezione adeguato ai dati personali trasferiti.

122. Emerge parimenti dalle osservazioni del commissario che la denuncia del sig. Schrems è volta a mettere direttamente in discussione la decisione 2000/520. Depositando tale denuncia, quest'ultimo ha inteso attaccare i termini e il funzionamento del regime dell'approdo sicuro in quanto tale, sulla base del rilievo che la sorveglianza di massa dei dati personali trasferiti negli Stati Uniti dimostrerebbe l'inesistenza di una protezione effettiva di tali dati nel diritto e nella prassi in vigore in tale paese terzo.

123. Inoltre, il giudice del rinvio osserva esso stesso che la garanzia offerta dall'articolo 7 della Carta e dai valori fondamentali comuni alle tradizioni costituzionali degli Stati membri sarebbe compromessa qualora si ammettesse che le comunicazioni elettroniche possano essere oggetto di accesso da parte delle autorità statali su base casuale e generaliz-

zata, senza che sia richiesta una motivazione oggettiva in base a considerazioni di sicurezza nazionale o prevenzione di crimini specificamente riguardanti i singoli soggetti interessati, e senza la previsione di garanzie adeguate e verificabili[47]. Il giudice del rinvio esprime pertanto indirettamente dei dubbi sulla validità della decisione 2000/520.

124. Per valutare se, nell'ambito del regime dell'approdo sicuro, gli Stati Uniti garantiscano un livello di protezione adeguato ai dati personali trasferiti è quindi necessario esaminare la validità di tale decisione.

125. A tal riguardo, occorre rilevare che, nell'ambito dello strumento di cooperazione fra la Corte e i giudici nazionali istituito dall'articolo 267 TFUE, la Corte, pur investita in via pregiudiziale esclusivamente di una questione di interpretazione del diritto dell'Unione, può, in talune circostanze particolari, essere indotta ad esaminare la validità di disposizioni di diritto derivato.

126. Pertanto, la Corte ha dichiarato d'ufficio, a più riprese, l'invalidità di un atto del quale le era stata chiesta soltanto l'interpretazione[48]. Essa ha parimenti statuito che «qualora risulti che le questioni deferite da un giudice nazionale abbiano in realtà ad oggetto la validità di atti [dell'Unione], la Corte è tenuta a pronunciarsi, senza imporre al giudice proponente un formalismo che servirebbe unicamente a ritardare il procedimento a norma dell'articolo [267 TFUE] e che sarebbe incompatibile con lo spirito dello stesso[49]». La Corte ha inoltre già dichiarato che i dubbi sollevati da un giudice del rinvio in merito alla compatibilità di un atto di diritto derivato con le norme volte alla tutela dei diritti fondamentali concernono la legittimità di tale atto sotto il profilo del diritto dell'Unione[50].

127. Ricordo parimenti che risulta dalla giurisprudenza della Corte che gli atti delle istituzioni, degli organi e degli organismi dell'Unione godono di una presunzione di validità, il che implica che essi producano effetti giuridici finché non siano stati revocati, annullati nel contesto di un ricorso per annullamento oppure dichiarati invalidi a seguito di un rinvio pregiudiziale o di un'eccezione di illegittimità. La Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, competenza che ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione. In mancanza di una declaratoria di invalidità, di modifica o di abrogazione da parte della Commissione, la decisione rimane obbligatoria in tutti i suoi elementi e direttamente applicabile in ogni Stato membro[51].

128. Al fine di fornire una risposta completa al giudice del rinvio e di fugare i dubbi espressi nel corso del presente procedimento in ordine alla validità della decisione 2000/520, ritengo che la Corte debba procedere ad una valutazione di validità di tale

[47] Punto 24 della decisione di rinvio.
[48] V., segnatamente, sentenze Strehl (62/76, EU:C:1977:18, punti da 10 a 17); Roquette Frères (145/79, EU:C:1980:234, punto 6), nonché Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, punti da 32 a 39).
[49] Sentenza Schwarze (16/65, EU:C:1965:117, pag. 1094).
[50] V. sentenza Hauer (44/79, EU:C:1979:290, punto 16).
[51] V., segnatamente, sentenza CIVAD (C-533/10, EU:C:2012:347, punti da 39 a 41 e la giurisprudenza ivi citata).

decisione.

129. Ciò premesso, occorre parimenti precisare che l'esame della questione se la decisione 2000/520 sia valida o meno deve essere circoscritto alle censure che sono state oggetto di discussione nell'ambito del presente procedimento. Infatti, in tale contesto non sono stati dibattuti tutti gli aspetti relativi al funzionamento del regime dell'approdo sicuro; per questo motivo, non mi sembra possibile dedicarmi in questa sede ad un esame esaustivo delle carenze di tale regime.

130. Per contro, la questione se l'accesso generalizzato e non mirato dei servizi americani di intelligence ai dati trasferiti sia idoneo ad incidere sulla legittimità della decisione 2000/520 è stata oggetto di discussione dinanzi alla Corte nell'ambito del presente procedimento. La validità di tale decisione può pertanto essere valutata sotto questo profilo.

B - *Sulla validità della decisione 2000/520*

1. Sugli elementi da prendere in considerazione per valutare la validità della decisione 2000/520

131. Occorre richiamare la giurisprudenza secondo la quale, «nell'ambito del ricorso per annullamento, la legittimità di un atto deve essere valutata in base alla situazione di fatto e di diritto esistente al momento in cui l'atto è stato adottato, e la valutazione della Commissione può essere criticata solo se essa risulta manifestamente erronea alla luce degli elementi di cui la stessa disponeva al momento dell'adozione dell'atto in questione[52] ».

132. Nella sentenza Gaz de France - Berliner Investissement[53], la Corte ha richiamato il principio secondo il quale «la valutazione della validità di un atto, che la Corte è tenuta ad effettuare nell'ambito di un rinvio pregiudiziale, deve normalmente essere fondata sulla situazione di fatto e di diritto esistente al momento in cui l'atto è stato adottato[54]». Sembra tuttavia che essa abbia ammesso che «la validità di un atto possa, in taluni casi, essere valutata in relazione ad elementi nuovi intervenuti dopo la sua adozione[55]».

133. Tale apertura così abbozzata dalla Corte mi sembra particolarmente rilevante nell'ambito della presente causa.

134. Infatti, le decisioni adottate dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46 presentano caratteristiche particolari. Esse sono destinate a valutare se il livello di protezione dei dati personali offerto da un paese terzo presenti o meno un carattere adeguato. Si tratta, in tal caso, di una valutazione destinata a mutare in funzione

[52] V., segnatamente, sentenza BVGD/Commissione (T-104/07 e T-339/08, EU:T:2013:366, punto 291), che richiama la sentenza IECC/Commissione (C-449/98 P, EU:C:2001:275, punto 87).

[53] C-247/08, EU:C:2009:600.

[54] Punto 49 e la giurisprudenza ivi citata.

[55] Punto 50 e la giurisprudenza ivi citata. V., in tal senso, Lenaerts, K., Maselis, I., e Gutman, K., EU *Procedural Law*, Oxford University Press, 2014, che enunciano che « in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court » (punto 10.16, pag. 471).

del contesto di fatto e di diritto vigente nel paese terzo.

135. Alla luce del fatto che la decisione di adeguatezza costituisce un tipo particolare di decisione, la regola secondo la quale la valutazione di validità della medesima potrebbe essere effettuata solo in funzione degli elementi esistenti al momento della sua adozione deve essere, nella specie, attenuata. Una siffatta regola comporterebbe altrimenti che, diversi anni dopo l'adozione di una decisione di adeguatezza, la valutazione sulla validità alla quale la Corte deve procedere non possa prendere in considerazione eventi che si sono verificati successivamente, e ciò sebbene un rinvio pregiudiziale per esame di validità non sia limitato nel tempo e il suo avvio possa appunto essere la conseguenza di fatti posteriori che rivelano le carenze dell'atto in questione.

136. Nella specie, il mantenimento in vigore della decisione 2000/520 da circa quindici anni dimostra che la Commissione ha implicitamente confermato la sua valutazione effettuata nel 2000. Quando, nell'ambito di un rinvio pregiudiziale, la Corte è indotta a vagliare la validità di una valutazione mantenuta nel tempo dalla Commissione, è dunque non solo possibile, ma anche appropriato, che essa possa rapportare tale valutazione alle circostanze nuove che sono intervenute dall'adozione della decisione di adeguatezza.

137. Tenuto conto della natura particolare della decisione di adeguatezza, quest'ultima deve essere oggetto di un riesame regolare da parte della Commissione. Se, a seguito di nuovi eventi verificatisi nel frattempo, la Commissione non modifica la propria decisione, essa conferma implicitamente, ma inevitabilmente, la valutazione effettuata all'inizio. Essa ribadisce pertanto la sua constatazione secondo la quale il paese terzo di cui trattasi assicura un livello di protezione adeguato ai dati personali trasferiti. Spetta alla Corte esaminare se tale constatazione continui ad essere valida malgrado le circostanze intervenute successivamente.

138. Al fine di assicurare un controllo giurisdizionale effettivo su questo tipo di decisione, la valutazione della sua validità deve pertanto essere effettuata, a mio avviso, tenendo conto del contesto di fatto e di diritto attuale.

2. Sulla nozione di livello di protezione adeguato

139. L'articolo 25 della direttiva 95/46 poggia interamente sul principio secondo il quale il trasferimento di dati personali verso un paese terzo può aver luogo soltanto se tale paese terzo garantisce un livello di protezione adeguato a tali dati. L'obiettivo di detto articolo consiste dunque nell'assicurare la continuità della protezione conferita da tale direttiva in caso di trasferimento di dati personali verso un paese terzo. Occorre rammentare, a tal riguardo, che detta direttiva offre un livello di protezione elevato dei cittadini dell'Unione con riguardo al trattamento dei loro dati personali.

140. Tenuto conto del ruolo importante svolto dalla protezione dei dati personali alla luce del diritto fondamentale al rispetto della vita privata, un siffatto livello elevato di protezione deve pertanto essere garantito, anche in caso di trasferimento di dati personali verso un paese terzo.

141. È per questo motivo che ritengo che la Commissione possa constatare, sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, che un paese terzo assicura un livello di protezione adeguato solo qualora, al termine di una valutazione di insieme del diritto

e della prassi nel paese terzo in questione, essa sia in grado di dimostrare che tale paese offre un livello di protezione sostanzialmente equivalente a quello offerto da tale direttiva, anche se le modalità di tale protezione possono essere diverse da quelle generalmente vigenti all'interno dell'Unione.

142. Benché il termine inglese «adequate» possa essere inteso, dal punto di vista linguistico, nel senso che esso designa un livello di protezione appena soddisfacente o sufficiente, ed avere pertanto un campo semantico diverso dal termine francese «adéquat», si deve osservare che il solo criterio che deve guidare l'interpretazione di tale termine è l'obiettivo consistente nel conseguimento di un livello elevato di protezione dei diritti fondamentali, come richiesto dalla direttiva 95/46.

143. L'esame del livello di protezione offerto da un paese terzo deve prendere in considerazione due elementi fondamentali, ossia il contenuto delle norme applicabili e i mezzi per assicurare il rispetto di tali norme[56].

144. A mio avviso, per conseguire un livello di protezione sostanzialmente equivalente a quello in vigore all'interno dell'Unione, il regime dell'approdo sicuro, il quale poggia in gran parte sull'autocertificazione e sull'autovalutazione da parte delle imprese che partecipano volontariamente a tale regime, dovrebbe essere accompagnato da garanzie adeguate e da un meccanismo di controllo sufficiente. Pertanto, i trasferimenti di dati personali verso paesi terzi non dovrebbero beneficiare di una protezione inferiore rispetto ai trattamenti effettuati all'interno dell'Unione.

145. A tal riguardo, rilevo, anzitutto, che all'interno dell'Unione prevale la concezione secondo la quale un dispositivo di controllo esterno sotto forma di un'autorità indipendente costituisce un elemento necessario di ogni sistema inteso ad assicurare il rispetto delle norme relative alla protezione dei dati personali.

146. Inoltre, al fine di assicurare l'effetto utile dell'articolo 25, paragrafi da 1 a 3, della direttiva 95/46, occorre tenere conto del fatto che l'adeguatezza del livello di protezione offerto da un paese terzo costituisce una situazione evolutiva che può mutare nel tempo in funzione di una serie di fattori. Gli Stati membri e la Commissione devono pertanto essere costantemente attenti ad ogni mutamento di circostanze idoneo a rendere necessaria una rivalutazione dell'adeguatezza del livello di protezione offerto da un paese terzo. Una valutazione dell'adeguatezza di tale livello di protezione non può affatto essere fissata ad un momento determinato e, poi, essere mantenuta indefinitamente, a prescindere da qualsiasi mutamento di circostanze che mostri che, in realtà, il livello di protezione offerto non è più adeguato.

147. L'obbligo del paese terzo di assicurare un livello di protezione adeguato costituisce pertanto un obbligo di durata. Pur se la valutazione è effettuata in un momento determinato, il mantenimento della decisione di adeguatezza presuppone che nessuna circostanza intervenuta successivamente sia in grado di rimettere in discussione la valutazione iniziale effettuata dalla Commissione.

[56] V. pag. 5 del documento di lavoro WP 12 della Commissione, intitolato «Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati , adottato dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali il 24 luglio 1998.

148. Infatti, non si deve perdere di vista il fatto che l'obiettivo dell'articolo 25 della direttiva 95/46 consiste nell'evitare che i dati personali vengano trasferiti verso un paese terzo che non assicura un livello di protezione adeguato, in violazione del diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta.

149. Occorre sottolineare che il potere conferito dal legislatore dell'Unione alla Commissione all'articolo 25, paragrafo 6, della direttiva 95/46, di constatare che un paese terzo assicura un livello di protezione adeguato, è espressamente subordinato alla necessità che tale paese terzo assicuri un tale livello ai sensi del paragrafo 2 di tale articolo. Qualora circostanze nuove siano idonee a rimettere in discussione la valutazione iniziale della Commissione, quest'ultima dovrebbe adeguare di conseguenza la propria decisione.

3. Valutazione

150. Ricordo che, ai sensi dell'articolo 25, paragrafo 6, della direttiva 95/46, «la Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona». Letto in combinato con l'articolo 25, paragrafo 2, di tale direttiva, l'articolo 25, paragrafo 6, della medesima significa che, per constatare che un paese terzo assicura un livello di protezione adeguato, la Commissione deve procedere ad una valutazione di insieme delle norme di diritto in vigore in tale paese terzo, nonché della loro applicazione.

151. Si è visto che il mantenimento, da parte della Commissione, della sua decisione 2000/520, malgrado il sopravvenire di elementi di fatto e di diritto nuovi, deve essere considerato espressione della volontà della medesima di confermare la sua valutazione iniziale.

152. Non spetta alla Corte, nell'ambito di un rinvio pregiudiziale, valutare i fatti all'origine della controversia che ha portato il giudice nazionale ad effettuare tale rinvio[57].

153. Mi baserò pertanto sui fatti indicati dal giudice del rinvio nella sua domanda di pronuncia pregiudiziale, fatti che, del resto, sono ampiamente considerati dimostrati dalla Commissione stessa[58].

154. Gli elementi che sono stati dedotti dinanzi alla Corte per contestare la valutazione della Commissione secondo la quale il regime dell'approdo sicuro assicura un livello di protezione adeguato ai dati personali trasferiti dall'Unione verso gli Stati Uniti possono essere così descritti.

[57] V., segnatamente, sentenza Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, punto 22 e la giurisprudenza ivi citata).

[58] V. comunicazione della Commissione menzionata alla nota a piè di pagina 2 e comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime «Approdo sicuro» dal punto di vista dei cittadini dell'UE e delle società ivi stabilite [COM(2013) 847 final].

155. Nella sua domanda di pronuncia pregiudiziale, il giudice del rinvio parte dalle due constatazioni di fatto seguenti. Da un lato, i dati personali trasferiti da imprese quali Facebook Ireland alla loro società madre stabilita negli Stati Uniti possono, successivamente, essere consultati dalla NSA nonché da altre agenzie di sicurezza americane nel corso di operazioni di sorveglianza e di intercettazioni massicce e indiscriminate. Infatti, a seguito delle rivelazioni del sig. Snowden, gli elementi di prova disponibili non ammettono attualmente altre conclusioni plausibili[59].
Dall'altro, i cittadini dell'Unione non disporrebbero di un diritto effettivo di essere sentiti sulla questione della sorveglianza e dell'intercettazione dei loro dati da parte della NSA e di altre agenzie di sicurezza americane[60].

156. Le constatazioni di fatto effettuate in tali termini dalla Corte d'appello sono suffragate dalle constatazioni effettuate dalla Commissione stessa.

157. Così, nella sua summenzionata comunicazione sul funzionamento del regime dell'approdo sicuro dal punto di vista dei cittadini dell'Unione e delle società ivi stabilite, la Commissione ha preso le mosse dalla constatazione che, nel corso del 2013, informazioni relative all'ampiezza e alla portata dei programmi di controllo americani hanno suscitato preoccupazioni sulla continuità della protezione dei dati personali lecitamente trasferiti negli USA nell'ambito del regime dell'approdo sicuro. Essa ha rilevato che tutte le imprese partecipanti al programma PRISM, e che consentono alle autorità americane di avere accesso a dati conservati e trattati negli Stati Uniti, risultano certificate nel quadro dell'approdo sicuro. A suo avviso, tale sistema è diventato così una delle piattaforme di accesso delle autorità americane di intelligence alla raccolta di dati personali inizialmente trattati nell'Unione[61].

158. Risulta da tali elementi che il diritto e la prassi degli Stati Uniti consentono di raccogliere su larga scala i dati personali di cittadini dell'Unione che vengono trasferiti nell'ambito del regime dell'approdo sicuro, senza che questi ultimi beneficino di una protezione giurisdizionale effettiva.

159. Tali constatazioni di fatto dimostrano, a mio avviso, che la decisione 2000/520 non contiene garanzie sufficienti. A causa di tale carenza di garanzie, detta decisione è stata attuata in un modo che non soddisfa i requisiti richiesti dalla Carta, nonché dalla direttiva 95/46.

160. Orbene, una decisione adottata dalla Commissione sul fondamento dell'articolo 25, paragrafo 6, della direttiva 95/46 è intesa alla constatazione che un paese terzo «garantisce» un livello di protezione adeguato. Il termine «garantisce», coniugato al presente, implica che, per potere essere mantenuta, una siffatta decisione deve riguardare un paese terzo che continua, successivamente all'adozione di detta decisione, a garantire un livello di protezione adeguato.

161. In realtà, le menzionate rivelazioni relative ai comportamenti della NSA, la quale utilizzerebbe dati trasferiti nell'ambito del regime dell'approdo sicuro, hanno evidenziato le debolezze della base giuridica costituita dalla decisione 2000/520.

[59] Punto 7, lettera *c)*, della decisione di rinvio.
[60] Punto 7, lettera *b)*, della decisione di rinvio.
[61] Pag. 19 della sua comunicazione.

162. Le carenze messe in evidenza nel corso del presente procedimento figurano più in particolare all'allegato I, quarto comma, di tale decisione. 163. Ricordo che, ai sensi di tale disposizione, «[l]'adesione [ai] principi [dell'approdo sicuro] può essere limitata: *a*) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; *b*) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione».

164. Il problema deriva sostanzialmente dall'impiego che le autorità americane fanno delle deroghe previste da detta disposizione. A causa della loro formulazione eccessivamente generica, l'attuazione di tali deroghe da parte di dette autorità non è limitata a quanto strettamente necessario.
165. A tale formulazione eccessivamente generica si somma la circostanza che i cittadini dell'Unione non dispongono di mezzi di ricorso adeguati avverso il trattamento dei loro dati personali per fini diversi da quelli per cui essi sono stati inizialmente raccolti e poi trasferiti verso gli Stati Uniti.

166. Le deroghe previste dalla decisione 2000/520 all'applicazione dei principi dell'approdo sicuro, segnatamente per esigenze legate alla sicurezza nazionale, avrebbero dovuto essere corredate dall'attuazione di un meccanismo di controllo indipendente idoneo ad evitare le violazioni al diritto alla vita privata accertate.

167. In tal senso, le rivelazioni sulla prassi dei servizi di intelligence americani quanto alla sorveglianza generalizzata dei dati trasferiti nell'ambito del regime dell'approdo sicuro hanno messo in luce talune carenze proprie della decisione 2000/520.

168. Le asserzioni nell'ambito della presente causa non integrano una violazione, da parte di Facebook, dei principi dell'approdo sicuro. Se un'impresa certificata, come Facebook USA, concede alle autorità americane l'accesso ai dati che le sono stati trasferiti da uno Stato membro, può ritenersi che essa lo faccia per conformarsi alla legislazione statunitense. Alla luce del fatto che una situazione del genere è espressamente ammessa dalla decisione 2000/520, a causa della formulazione ampia delle deroghe che essa contiene, è in realtà la questione della compatibilità di tali deroghe con il diritto primario dell'Unione a porsi nell'ambito della presente causa.

169. Occorre sottolineare, a tal riguardo, che si evince da una giurisprudenza costante della Corte che il rispetto dei diritti dell'uomo rappresenta una condizione di legittimità degli atti dell'Unione e che nell'Unione non possono essere consentite misure incompatibili con il rispetto di questi ultimi[62].

170. Risulta peraltro dalla giurisprudenza della Corte che la comunicazione dei dati personali raccolti a terzi, pubblici o privati, costituisce un'ingerenza nel diritto al rispetto

[62] V., segnatamente, sentenza Kadi e Al Barakaat International Foundation/Consiglio e Commissione (C-402/05 P e C-415/05 P, EU:C:2008:461, punto 284, nonché la giurisprudenza ivi citata).

della vita privata «quale che sia l'ulteriore utilizzazione delle informazioni così comunicate[63]». Ancora, nella sentenza Digital Rights Ireland e a.[64], la Corte ha confermato che il fatto di autorizzare le autorità nazionali competenti ad avere accesso a siffatti dati costituisce un pregiudizio supplementare a tale diritto fondamentale[65]. Inoltre, qualsiasi forma di trattamento dei dati personali è prevista all'articolo 8 della Carta e costituisce un'ingerenza nel diritto alla protezione di tali dati[66]. L'accesso di cui dispongono i servizi di intelligence americani ai dati trasferiti integra pertanto parimenti un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito dall'articolo 8 della Carta, in quanto un siffatto accesso costituisce un trattamento di tali dati.

171. Come constatato dalla Corte in tale sentenza, l'ingerenza così individuata è di vasta portata e va considerata particolarmente grave, alla luce del numero significativo di utenti interessati e delle quantità di dati trasferiti. Tali elementi, sommati alla segretezza dell'accesso da parte delle autorità americane ai dati personali trasferiti verso le imprese stabilite negli Stati Uniti, rendono l'ingerenza estremamente seria.

172. A ciò si aggiunge la circostanza che i cittadini dell'Unione utenti di Facebook non sono informati del fatto che i loro dati personali saranno accessibili in maniera generale per le agenzie di sicurezza americane.

173. Occorre parimenti porre l'accento sul fatto che il giudice del rinvio ha constatato che, negli Stati Uniti, i cittadini dell'Unione non hanno alcun diritto effettivo ad essere sentiti sulla questione della sorveglianza e dell'intercettazione dei loro dati. La FISC esercita una supervisione, ma il procedimento dinanzi alla medesima è segreto e si svolge inaudita altera parte[67]. Ritengo che si sia in presenza, in tal caso, di un'ingerenza nel diritto dei cittadini dell'Unione ad un ricorso effettivo, tutelato dall'articolo 47 della Carta.

174. Sussiste pertanto un'ingerenza nei diritti fondamentali tutelati dagli articoli 7, 8 e 47 della Carta resa possibile dalle deroghe ai principi dell'approdo sicuro di cui all'allegato I, quarto comma, della decisione 2000/520.

175. Occorre adesso verificare se tale ingerenza sia giustificata o meno.

176. Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti da quest'ultima devono essere previste dalla legge e devono rispettare il contenuto essenziale di tali diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni a detti diritti e libertà solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

177. Alla luce delle condizioni così fissate per poter ammettere limitazioni all'esercizio dei diritti e delle libertà protetti dalla Carta, dubito fortemente che si possa ritenere che le limitazioni oggetto della presente causa rispettino il contenuto essenziale degli articoli 7 e

[63] Sentenza Österreichischer Rundfunk e a. (C-465/00, C-138/01 e C-139/01, EU:C:2003:294, punto 74).
[64] C-293/12 e C-594/12, EU:C:2014:238.
[65] Punto 35.
[66] Punto 36
[67] Punto 7, lettera *b)*, della decisione di rinvio.

8 della Carta. Infatti, l'accesso dei servizi di intelligence americani ai dati trasferiti sembra estendersi al contenuto delle comunicazioni elettroniche; ciò arrecherebbe pregiudizio al contenuto essenziale del diritto fondamentale al rispetto della vita privata e degli altri diritti sanciti all'articolo 7 della Carta. Inoltre, nella misura in cui la formulazione ampia delle limitazioni previste all'allegato I, quarto comma, della decisione 2000/520 consente potenzialmente di disapplicare l'insieme dei principi dell'approdo sicuro, si potrebbe ritenere che tali limitazioni pregiudichino il contenuto essenziale del diritto fondamentale alla protezione dei dati personali[68].

178. Quanto alla questione se l'ingerenza constatata risponda ad un obiettivo di interesse generale, ricordo, anzitutto, che, ai sensi dell'allegato I, quarto comma, lettera *b*), della decisione 2000/520, l'adesione ai principi dell'approdo sicuro può essere limitata «da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione».

179. È giocoforza constatare che i «legittimi interessi» menzionati in tale disposizione non vengono precisati. Ne risulta un'incertezza quanto all'ambito di applicazione, potenzialmente estremamente ampio, di tale deroga all'applicazione dei principi dell'approdo sicuro da parte delle imprese aderenti.

180. La lettura delle spiegazioni contenute al titolo B dell'allegato IV della decisione 2000/520, intitolato «Autorizzazioni legali esplicite», conferma tale impressione, in particolare l'affermazione secondo la quale «[è] ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi "approdo sicuro", devono osservare la legge». Viene inoltre indicato, per quanto attiene alle autorizzazioni esplicite, che «sebbene i principi "approdo sicuro" intendano colmare le differenze tra il sistema americano e quello europeo relativamente alla tutela della privacy, siamo tenuti al rispetto delle prerogative legislative dei legislatori eletti».

181. Ne risulta che, a mio avviso, tale deroga è contraria agli articoli 7, 8 e 52, paragrafo 1, della Carta, nella misura in cui essa non persegue un obiettivo di interesse generale definito in maniera sufficientemente precisa.

182. In ogni caso, la facilità e la genericità con le quali la stessa decisione 2000/520, ai suoi allegati I, quarto comma, lettera *b*), e IV, B, prevede che i principi dell'approdo sicuro possano essere esclusi in applicazione di norme di diritto americano sono incompatibili con la condizione secondo la quale le deroghe alle norme relative alla protezione dei dati personali devono essere limitate a quanto strettamente necessario.
Il requisito della necessità viene effettivamente menzionato, ma, a parte il fatto che la dimostrazione di tale requisito è posta a carico dell'impresa di cui trattasi, non vedo come una siffatta impresa potrebbe sottrarsi ad un obbligo di escludere i principi dell'approdo sicuro che discende da norme di diritto che essa è tenuta ad applicare.

183. Ritengo pertanto che la decisione 2000/520 debba essere dichiarata invalida per-

[68] V., a tal riguardo, sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punti 39 e 40).

ché l'esistenza di una deroga che consente in maniera talmente generica e imprecisa di escludere i principi del regime dell'approdo sicuro impedisce di per sé di ritenere che tale regime garantisca un livello di protezione adeguato ai dati personali che vengono trasferiti negli Stati Uniti dall'Unione.

184. Passando poi alla prima categoria di limiti previsti all'allegato I, quarto comma, lettera *a*), della decisione 2000/520, attinenti ad esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia degli Stati Uniti, solo la prima finalità mi sembra essere sufficientemente precisa da essere considerata una finalità di interesse generale riconosciuta dall'Unione ai sensi dell'articolo 52, paragrafo 1, della Carta.

185. Occorre adesso verificare la proporzionalità dell'ingerenza constatata.
186. A questo proposito, si deve ricordare che il «principio di proporzionalità esige, secondo una costante giurisprudenza della Corte, che gli atti delle istituzioni dell'Unione siano idonei a realizzare gli obiettivi legittimi perseguiti dalla normativa di cui trattasi e non superino i limiti di ciò che è idoneo e necessario al conseguimento degli obiettivi stessi[69]».

187. Per quanto riguarda il controllo giurisdizionale del rispetto di tali condizioni, «allorché si tratta di ingerenze in diritti fondamentali, la portata del potere discrezionale del legislatore dell'Unione può risultare limitata in funzione di un certo numero di elementi, tra i quali figurano, in particolare, il settore interessato, la natura del diritto di cui trattasi garantito dalla Carta, la natura e la gravità dell'ingerenza nonché la finalità di quest'ultima[70]».

188. Ritengo che le decisioni adottate dalla Commissione sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46 siano integralmente soggette al controllo della Corte quanto alla proporzionalità della valutazione effettuata da tale istituzione in merito all'adeguatezza del livello di protezione offerto da un paese terzo a causa «della sua legislazione nazionale o dei suoi impegni internazionali».

189. Occorre osservare a tal riguardo che, nella sentenza Digital Rights Ireland e a.[71], la Corte ha dichiarato che, «tenuto conto, da un lato, del ruolo importante svolto dalla protezione dei dati personali sotto il profilo del diritto fondamentale al rispetto della vita privata e, dall'altro, della portata e della gravità dell'ingerenza in tale suddetto diritto che la direttiva [in questione] comporta, il potere discrezionale del legislatore dell'Unione risulta ridotto e di conseguenza è necessario procedere ad un controllo stretto[72]» .

190. Una siffatta ingerenza deve essere idonea a realizzare l'obiettivo perseguito dall'atto dell'Unione in questione ed essere necessaria a conseguire tale obiettivo.

191. A tal riguardo, «[p]er quel che riguarda il rispetto della vita privata, la protezione di tale diritto fondamentale, secondo la costante giurisprudenza della Corte, richiede […] che le deroghe e le restrizioni alla tutela dei dati personali debbano operare entro i limiti

[69] Sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 46, nonché la giurisprudenza ivi citata).
[70] *Ibidem* (punto 47 e la giurisprudenza ivi citata).
[71] C-293/12 e C-594/12 , EU:C:2014:238.
[72] Punto 48.

dello stretto necessario[73]».

192. Nel suo controllo, la Corte tiene parimenti conto della circostanza che «la tutela dei dati personali, risultante dall'obbligo esplicito previsto all'articolo 8, paragrafo 1, della Carta, riveste un'importanza particolare per il diritto al rispetto della vita privata sancito dall'articolo 7 della stessa[74]».

193. Secondo la Corte, la quale richiama, a tal riguardo, la giurisprudenza della Corte europea dei diritti dell'uomo, «la normativa dell'Unione di cui trattasi deve prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura de qua e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati[75]». La Corte indica che «[l]a necessità di disporre di siffatte garanzie è tanto più importante allorché […] i dati personali sono soggetti a trattamento automatico ed esiste un rischio considerevole di accesso illecito ai dati stessi[76]».

194. Esiste, a mio avviso, un'analogia fra l'allegato I, quarto comma, lettera *a*), della decisione 2000/520 e l'articolo 13, paragrafo 1, della direttiva 95/46. Nella prima disposizione, è indicato che l'adesione ai principi dell'approdo sicuro può essere limitata «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]». Nella seconda, viene previsto che gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni dell'articolo 6, paragrafo 1, dell'articolo 10, dell'articolo 11, paragrafo 1 e degli articoli 12 e 21 di tale direttiva, qualora tale restrizione costituisca una misura necessaria alla salvaguardia, segnatamente, della sicurezza dello Stato, della difesa, della pubblica sicurezza, nonché della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali.

195. Come rilevato dalla Corte nella sua sentenza IPI[77], dal dettato dell'articolo 13, paragrafo 1, della direttiva 95/46 risulta che gli Stati membri possono prevedere le misure contemplate da tale disposizione unicamente quando siano necessarie. La «necessità» delle misure condiziona quindi la facoltà accordata agli Stati membri da detta disposizione[78]. In relazione ai trattamenti di dati personali all'interno dell'Unione, deve ritenersi che i limiti previsti dall'articolo 13 di tale direttiva siano circoscritti a quanto strettamente necessario al conseguimento dell'obiettivo perseguito. Lo stesso deve valere, a mio avviso, nel caso dei limiti ai principi dell'approdo sicuro che sono previsti all'allegato I, quarto comma, della decisione 2000/520.

196. Orbene, è giocoforza constatare che non tutte le versioni linguistiche menzionano il criterio della necessità nel testo dell'allegato I, quarto comma, lettera *a*), della decisione

[73] Sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 52, nonché la giurisprudenza ivi citata).
[74] *Ibidem* (punto 53).
[75] *Ibidem* (punto 54 e la giurisprudenza ivi citata).
[76] *Ibidem* (punto 55 e la giurisprudenza ivi citata).
[77] C-473/12, EU:C:2013:715
[78] Punto 32.

2000/520. Ciò vale, segnatamente, per la versione in lingua francese, la quale indica che «[l]'adhésion aux principes peut être limitée par […] les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis», mentre, a titolo di esempio, le versioni in lingua spagnola, tedesca e inglese indicano che le limitazioni istituite devono essere necessarie per conseguire gli obiettivi summenzionati.

197. In ogni caso, gli elementi di fatto dedotti dal giudice del rinvio, nonché dalla Commissione nelle sue summenzionate comunicazioni mostrano chiaramente che, nella prassi, l'attuazione di tali limitazioni non è circoscritta a quanto strettamente necessario al conseguimento degli obiettivi previsti.

198. Osservo, a tal proposito, che l'accesso ai dati personali trasferiti di cui dispongono i servizi di intelligence americani copre in maniera generale qualsiasi persona e qualsiasi mezzo di comunicazione elettronica, nonché l'insieme dei dati trasferiti, compreso il contenuto delle comunicazioni senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di interesse generale perseguito[79].

199. Infatti, l'accesso dei servizi di intelligence americani ai dati trasferiti riguarda in maniera globale l'insieme delle persone che fanno uso dei servizi di comunicazione elettronica, senza che sia richiesto che le persone interessate presentino una minaccia per la sicurezza nazionale[80].

200. Una siffatta sorveglianza massiccia e indifferenziata è sproporzionata per natura e costituisce un'ingerenza ingiustificata nei diritti garantiti dagli articoli 7 e 8 della Carta.

201. Come rilevato giustamente dal Parlamento nelle sue osservazioni, poiché è impossibile, per il legislatore dell'Unione o per gli Stati membri, adottare disposizioni legislative che, in violazione, della Carta, prevedano una sorveglianza massiccia e indifferenziata, ne consegue inevitabilmente e a maggior ragione che non si può ritenere in alcuna circostanza che paesi terzi garantiscano un livello di protezione adeguato ai dati personali dei cittadini dell'Unione allorché la loro normativa autorizza effettivamente la sorveglianza e l'intercettazione massicce e indifferenziate di questo tipo di dati.

202. Occorre inoltre sottolineare che il regime dell'approdo sicuro, come definito dalla decisione 2000/520, non contiene le garanzie idonee ad evitare un accesso massiccio e generalizzato ai dati trasferiti.

203. Osservo, a tal riguardo, che la Corte ha messo in evidenza, nella sentenza Digital Rights Ireland e a.[81], l'importanza di prevedere «norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta[82]». Secondo la Corte, una siffatta ingerenza deve essere «regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario[83]». La Corte ha parimenti posto l'accento, in questa sentenza, sulla necessità di

[79] V., per analogia, sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 57 e la giurisprudenza ivi citata).
[80] *Ibidem* (punti 58 e 59).
[81] C-293/12 e C-594/12 , EU:C:2014:238.
[82] Punto 65.
[83] *Idem*.

prevedere « garanzie sufficienti, come richieste dall'articolo 8 della Carta, che permettano di assicurare una protezione efficace dei dati [personali] conservati contro i rischi di abuso nonché contro eventuali accessi e usi illeciti dei suddetti dati[84]».

204. Orbene, è giocoforza constatare che i meccanismi di arbitrato privato e la FTC, a causa del suo ruolo limitato alle controversie di natura commerciale, non costituiscono strumenti di contestazione dell'accesso dei servizi di intelligence americani ai dati personali trasferiti dall'Unione.

205. La competenza della FTC è limitata agli atti e alle pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, ed essa non si estende pertanto alla raccolta e all'impiego di informazioni personali a fini non commerciali[85]. L'ambito di competenza limitato della FTC restringe il diritto dei singoli alla protezione dei loro dati personali. La FTC è stata creata non già per assicurare la protezione del diritto individuale alla vita privata, come avviene in seno all'Unione per le autorità nazionali di controllo, bensì per garantire un commercio leale ed affidabile per i consumatori, il che limita, de facto, le sue capacità di intervento nella sfera relativa alla protezione dei dati personali. La FTC non svolge pertanto un ruolo equiparabile a quello delle autorità nazionali di controllo previste all'articolo 28 della direttiva 95/46.

206. I cittadini dell'Unione i cui dati sono stati trasferiti possono rivolgersi ad organismi arbitrali specializzati stabiliti negli Stati Uniti, come TRUSTe e BBBOnline, per chiedere precisazioni sulla questione se l'impresa che detiene i loro dati personali violi i requisiti del regime di autocertificazione. L'arbitrato privato assicurato da organismi come TRUSTe non può trattare le violazioni del diritto alla protezione dei dati personali commesse da organismi o autorità diverse dalle imprese autocertificate. Tali organismi arbitrali non hanno alcuna competenza a statuire sulla legittimità delle attività delle agenzie di sicurezza americane.

207. Né la FTC né gli organismi arbitrali privati sono pertanto competenti a controllare le possibili violazioni dei principi di protezione dei dati personali commesse da operatori pubblici come le agenzie di sicurezza americane. Una siffatta competenza sarebbe tuttavia essenziale per garantire pienamente il diritto alla protezione effettiva di tali dati. La Commissione non poteva pertanto constatare, adottando la decisione 2000/520 e mantenendola in vigore, che per l'insieme dei dati personali trasferiti verso gli Stati Uniti sussistesse una protezione adeguata del diritto conferito dall'articolo 8, paragrafo 3, della Carta, ossia che un'autorità indipendente esercitasse un controllo effettivo sul rispetto dei requisiti di protezione e sicurezza di tali dati.

208. Occorre pertanto rilevare l'assenza, nel regime dell'approdo sicuro previsto dalla decisione 2000/520, di un'autorità indipendente che possa controllare che l'attuazione delle deroghe ai principi dell'approdo sicuro venga limitata allo stretto necessario. Orbene, si è visto che un siffatto controllo da parte di un'autorità indipendente costituisce, sotto il profilo del diritto dell'Unione, un elemento essenziale del rispetto della tutela delle perso-

[84] *Ibidem* (punto 66).

[85] V., a tal riguardo, allegato II, FAQ 11, della decisione 2000/520, *sub* «Attività della Commissione federale per il commercio (Federal Trade Commission, FTC)», e allegati III, V e VII alla medesima.

ne con riguardo al trattamento dei dati personali[86].

209. Occorre sottolineare, a tal riguardo, il ruolo svolto, nel sistema di protezione dei dati personali in vigore all'interno dell'Unione, dalle autorità nazionali di controllo in sede di controllo delle limitazioni previste all'articolo 13 della direttiva 95/46. Ai sensi dell'articolo 28, paragrafo 4, secondo comma, di tale direttiva, «[q]ualsiasi persona può, in particolare, chiedere a un'autorità di controllo di verificare la liceità di un trattamento quando si applicano le disposizioni nazionali adottate a norma dell'articolo 13 della presente direttiva ». Per analogia, ritengo che la menzione di limiti all'applicazione dei principi dell'approdo sicuro all'allegato I, quarto comma, della decisione 2000/520, avrebbe dovuto essere accompagnata dall'attuazione di un meccanismo di controllo assicurato da un'autorità indipendente specializzata in materia di protezione dei dati personali.

210. L'intervento di autorità di controllo indipendenti si trova, infatti, al centro del sistema europeo di protezione dei dati personali. È pertanto naturale che l'esistenza di siffatte autorità sia stata considerata, anzitutto, una delle condizioni necessarie alla constatazione dell'adeguatezza del livello di protezione offerto dai paesi terzi. Si tratta di una condizione affinché i flussi di dati dal territorio degli Stati membri verso quello di paesi terzi non vengano vietati in conformità all'articolo 25 della direttiva 95/46[87]. Come rilevato nel documento di discussione adottato dal gruppo di lavoro istituito dall'articolo 29 di tale direttiva, vi è in Europa un ampio consenso sulla necessità di «un sistema di "controllo esterno" sotto forma di autorità indipendente, atto ad assicurare l'osservanza delle norme di tutela[88]».

211. Rilevo, inoltre, che la FISC non mette a disposizione dei cittadini dell'Unione i cui dati personali sono stati trasferiti negli Stati Uniti un ricorso giurisdizionale effettivo. Infatti, le tutele nei confronti della sorveglianza posta in essere dai servizi governativi nell'ambito dell'articolo 702 della legge del 1978 sulla sorveglianza dei servizi di intelligence stranieri si applicano unicamente ai cittadini americani, nonché ai cittadini stranieri che risiedono legalmente e permanentemente negli Stati Uniti. Come rilevato dalla Commissione stessa, il controllo dei programmi americani di raccolta di intelligence potrebbe essere migliorato rafforzando il ruolo della FISC e introducendo mezzi di ricorso per i singoli. Questi meccanismi potrebbero ridurre il trattamento di dati personali dei cittadini dell'Unione che non sono rilevanti ai fini della protezione della sicurezza nazionale[89].

212. Inoltre, la Commissione ha indicato essa stessa che i cittadini dell'Unione non hanno alcuna possibilità di ottenere l'accesso, la rettifica o la cancellazione dei dati, o rimedi amministrativi o giurisdizionali in relazione alla raccolta e all'ulteriore trattamento dei

[86] V. sentenza Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238, punto 68, nonché la giurisprudenza ivi citata).
[87] V. POULLET, Y., «L'autorité de contrôle: 'vues' de Bruxelles», *Revue française d'administration publique*, n. 89, gennaiomarzo 1999, pag. 69, specialmente pag. 71.
[88] V. pag. 7 del documento di lavoro WP 12 della Commissione menzionato alla nota a piè di pagina 56.
[89] Pagg. 10 e 11 della comunicazione della Commissione menzionata alla nota a piè di pagina 2.

loro dati personali nell'ambito dei programmi di controllo americani[90].

213. Occorre infine rilevare che le norme americane relative alla protezione della vita privata possono essere oggetto di un'applicazione differenziata fra i cittadini americani e i cittadini stranieri[91].

214. Da quanto precede deriva che la direttiva 2000/520 non prevede norme chiare e precise che regolino la portata dell'ingerenza nei diritti fondamentali sanciti dagli articoli 7 e 8 della Carta. È quindi giocoforza constatare che tale decisione e l'applicazione che ne viene fatta comportano un'ingerenza di vasta portata e di particolare gravità in detti diritti fondamentali, senza che siffatta ingerenza sia regolamentata con precisione da disposizioni che permettano di garantire che essa sia effettivamente limitata a quanto strettamente necessario.

215. Adottando la decisione 2000/520, e poi mantenendola in vigore, la Commissione ha dunque oltrepassato i limiti imposti dal rispetto del principio di proporzionalità alla luce degli articoli 7, 8 e 52, paragrafo 1, della Carta. A ciò si aggiunge la constatazione di un'ingerenza ingiustificata nel diritto dei cittadini dell'Unione ad un ricorso effettivo, tutelato dall'articolo 47 della Carta.

216. Di conseguenza, tale decisione deve essere dichiarata invalida, dato che, a causa delle violazioni dei diritti fondamentali descritte in precedenza, non può ritenersi che il regime dell'approdo sicuro da essa instaurato garantisca un livello di protezione adeguato ai dati personali che vengono trasferiti dall'Unione verso gli Stati Uniti nell'ambito di tale regime.

217. A fronte di una siffatta constatazione di violazioni dei diritti fondamentali dei cittadini dell'Unione, ritengo che la Commissione avrebbe dovuto sospendere l'applicazione della decisione 2000/520.

218. Tale decisione ha una durata indeterminata. Orbene, la presente causa dimostra che l'adeguatezza del livello di protezione offerto da un paese terzo può evolversi nel tempo in funzione del mutamento delle circostanze sia di fatto che di diritto che hanno fondato detta decisione.

219. Rilevo che la stessa decisione 2000/520 contiene disposizioni che prevedono la possibilità per la Commissione di adeguare la medesima in funzione delle circostanze.

220. In tal senso, risulta dal considerando 9 di tale decisione che «[l]'approdo sicuro creato dai principi e dalle FAQ può richiedere una revisione alla luce dell'esperienza e degli sviluppi riguardanti la tutela della vita privata in un contesto in cui la tecnologia rende sempre più facile il trasferimento e il trattamento dei dati personali, e dei risultati delle attività di applicazione e di esecuzione da parte delle autorità competenti».

[90] Punto 7.2, pag. 20, della comunicazione della Commissione menzionata alla nota a piè di pagina a pag. 58.

[91] V., su tale questione, KUNER, C., «Foreign Nationals and Data Protection Law: A Transatlantic Analysis», *Data Protection Anno 2014: How To Restore Trust?* Intersentia, Cambridge, 2014, pag. 213, specialmente pag. 216 e segg.

221. Analogamente, ai sensi dell'articolo 3, paragrafo 4, di detta decisione, «[o]ve le informazioni di cui ai paragrafi 1, 2 e 3 del presente articolo provino che uno degli organismi incaricati di garantire la conformità ai principi applicati conformemente alle FAQ negli Stati Uniti non svolge la sua funzione in modo efficace, la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure […] al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione».

222. Inoltre, secondo l'articolo 4, paragrafo 1, della decisione 2000/520, essa «può essere adattata in qualsiasi momento alla luce dell'esperienza acquisita nella sua attuazione e/o qualora il livello di protezione offerta dai principi e dalle FAQ sia superato dai requisiti della legislazione degli Stati Uniti. La Commissione valuta in ogni caso l'applicazione della presente decisione tre anni dopo la sua notifica agli Stati membri sulla base delle informazioni disponibili e comunica qualsiasi riscontro al comitato istituito dall'articolo 31 della direttiva 95/46/[...], fornendo altresì ogni indicazione che possa influire sulla valutazione relativa all'adeguata salvaguardia offerta dalla disposizione di cui all'articolo 1 della presente decisione, ai sensi dell'articolo 25 della direttiva 95/46». Ai sensi dell'articolo 4, paragrafo 2, della decisione 2000/520, «[l]a Commissione, se necessario, presenta progetti di opportuni provvedimenti in conformità alla procedura di cui all'articolo 31 della direttiva 95/46».

223. La Commissione ha rilevato, nelle sue osservazioni, che «esiste un'elevata probabilità che l'adesione ai principi dell'approdo sicuro sia stata limitata in un modo che non risponde più alle condizioni strettamente circoscritte dell'esenzione prevista in materia di sicurezza nazionale[92]». Essa osserva, a tal riguardo, che «[dall]e rivelazioni in questione emerge un grado di sorveglianza indifferenziata su larga scala, il quale non è compatibile con il criterio di necessità previsto in tale esenzione né, in termini più generali, con il diritto alla protezione dei dati personali sancito all'articolo 8 della Carta[93]». La Commissione ha inoltre constatato essa stessa che «[l]a portata [dei] programmi di controllo, associata alla disparità di trattamento riservata ai cittadini [dell'Unione], mette in questione il livello di protezione offerto dall'accordo Approdo sicuro[94]».

224. Inoltre, la Commissione ha espressamente riconosciuto, in udienza, che, nell'ambito della decisione 2000/520, come è applicata attualmente, non sussistono garanzie che il diritto dei cittadini dell'Unione alla protezione dei loro dati sarà assicurato. Tale constatazione non è tuttavia idonea, a suo avviso, a rendere invalida tale decisione. Pur se la Commissione condivide l'affermazione secondo la quale essa deve agire a fronte di circostanze nuove, essa ritiene di avere adottato misure adeguate e proporzionate avviando negoziati con gli Stati Uniti al fine di riformare il regime dell'approdo sicuro.

225. Non sono di tale avviso. Infatti, nel frattempo, i trasferimenti di dati personali verso gli Stati Uniti devono poter essere sospesi su iniziativa delle autorità nazionali di controllo o a seguito di denunce depositate presso le medesime.

226. Inoltre, ritengo che, a fronte di tali constatazioni, la Commissione avrebbe dovuto sospendere l'applicazione della decisione 2000/520. Infatti, l'obiettivo di protezione dei

[92] Punto 44.
[93] *Idem*.
[94] Pag. 5 della comunicazione della Commissione menzionata alla nota a piè di pagina 2.

dati personali perseguito dalla direttiva 95/46 nonché dall'articolo 8 della Carta fa gravare taluni obblighi non solo sugli Stati membri, ma anche sulle istituzioni dell'Unione, come risulta dall'articolo 51, paragrafo 1, della Carta.

227. Nella sua valutazione del livello di protezione offerto da un paese terzo, la Commissione deve esaminare non solo la normativa interna e gli impegni internazionali di tale paese terzo, ma anche il modo in cui la protezione dei dati personali viene garantita nella prassi. Se l'esame della prassi rivela delle disfunzioni, la Commissione deve reagire e, se del caso, sospendere e/o adeguare senza indugio la propria decisione.

228. Come si è visto nelle considerazioni svolte in precedenza, l'obbligo incombente sugli Stati membri consiste principalmente nell'assicurare, tramite l'azione delle loro autorità nazionali di controllo, il rispetto delle norme previste dalla direttiva 95/46.

229. L'obbligo che grava sulla Commissione consiste nel sospendere l'applicazione di una decisione da essa adottata sulla base dell'articolo 25, paragrafo 6, di tale direttiva in caso di comprovati inadempimenti da parte del paese terzo di cui trattasi fintantoché essa conduce negoziati con tale paese terzo onde porre fine a detti inadempimenti.

230. Ricordo che una decisione adottata dalla Commissione sulla base di tale disposizione è intesa a constatare che un paese terzo «garantisce» un livello di protezione adeguato ai dati personali oggetto di un trasferimento verso tale paese terzo. Il termine «garantisce», coniugato al presente, implica che, per poter essere mantenuta, una siffatta decisione debba riguardare un paese terzo che, successivamente all'adozione di detta decisione, continua a garantire un siffatto livello di protezione adeguato.

231. Secondo il considerando 57 della direttiva 95/46, «deve essere vietato il trasferimento di dati personali verso un paese terzo che non offre un livello di protezione adeguato».

232. Ai sensi dell'articolo 25, paragrafo 4, di tale direttiva, «[q]ualora la Commissione constati, secondo la procedura dell'articolo 31, paragrafo 2, che un paese terzo non garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il paese terzo in questione». Inoltre, l'articolo 25, paragrafo 5, di detta direttiva dispone che «[l]a Commissione avvia, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione di cui al paragrafo 4».

233. Risulta da quest'ultima disposizione che, nel sistema predisposto dall'articolo 25 della direttiva 95/46, i negoziati avviati con un paese terzo sono volti a rimediare ad un'assenza di livello di protezione adeguato constatata in conformità al procedimento previsto all'articolo 31, paragrafo 2, di tale direttiva. Nel caso di specie, la Commissione non ha formalmente constatato, in conformità a tale procedura, che il regime dell'approdo sicuro non garantiva più un livello di protezione adeguato. Ciò premesso, se la Commissione ha deciso di avviare negoziati con gli Stati Uniti, è proprio perché essa ha ritenuto, in via preliminare, che il livello di protezione assicurato da questo paese terzo non fosse più adeguato.

234. Sebbene fosse a conoscenza di disfunzioni in sede di applicazione della decisione 2000/520, la Commissione non ha né sospeso né adeguato quest'ultima, determinando

in tal modo il persistere della violazione dei diritti fondamentali delle persone i cui dati personali sono stati e continuano ad essere trasferiti nell'ambito del regime dell'approdo sicuro.

235. Orbene, la Corte ha già dichiarato, pur se in un altro contesto, che spetta alla Commissione vigilare sull'adeguamento di una normativa ai nuovi dati[95].

236. Una siffatta inerzia della Commissione, che arreca direttamente pregiudizio ai diritti fondamentali tutelati dagli articoli 7, 8 e 47 della Carta, costituisce, a mio avviso, un motivo supplementare per dichiarare invalida la decisione 2000/520 nell'ambito del presente rinvio pregiudiziale[96].

III – Conclusione

237. Sulla scorta delle considerazioni sin qui svolte, propongo alla Corte di risolvere nel modo seguente le questioni pregiudiziali sottopostele dalla Corte d'appello: L'articolo 28 della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, in combinato con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che l'esistenza di una decisione adottata dalla Commissione europea sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46 non produce l'effetto di impedire ad un'autorità nazionale di controllo di istruire una denuncia con la quale si lamenta che un paese terzo non garantisce un livello di protezione adeguato ai dati personali trasferiti e, se del caso, di sospendere il trasferimento di tali dati. La decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, è invalida.

[95] V., in tal senso, sentenza Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, punto 40).

[96] Sebbene la Corte abbia dichiarato, nella sentenza T. Port (C-68/95, EU:C:1996:452) che «il Trattato non ha previsto la possibilità di un rinvio con cui il giudice nazionale chieda alla Corte di dichiarare in via pregiudiziale la carenza di un'istituzione» (punto 53), sembra che essa adotti una posizione più favorevole a tale possibilità nella sentenza Ten Kate Holding Musselkanaal e a. (C-511/03, EU:C:2005:625, punto 29).

ROMA TRE
UNIVERSITÀ DEGLI STUDI

La Corte di Giustizia dell'Unione Europea sta intervenendo in maniera crescente nel campo della protezione dei dati personali.

La decisione nel caso Schrems segna un ulteriore passo verso l'affermazione di un modello europeo contrapposto a quello statunitense e la primazia del controllo giudiziario sugli accordi UE/USA.

Il volume si pone in continuità rispetto a quello sulla precedente sentenza nel caso Google Spain [Roma TrE-Press 2015]: dodici studiosi analizzano la nuova decisione sotto molteplici aspetti giuridici, prospettando interpretazioni e prospettive anche alla luce del "Privacy Shield" che dovrebbe governare la circolazione trans-atlantica dei dati.

Roma TrE-Press
2016